

ClientSPB

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.5.55/28

Шлюз 100.70.5.49

DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru

Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
100.70.5.55	28	100.70.5.49

Add Delete

DNS servers: 100.100.100.100

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

VDS

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.6.12/29

Шлюз 100.70.6.9

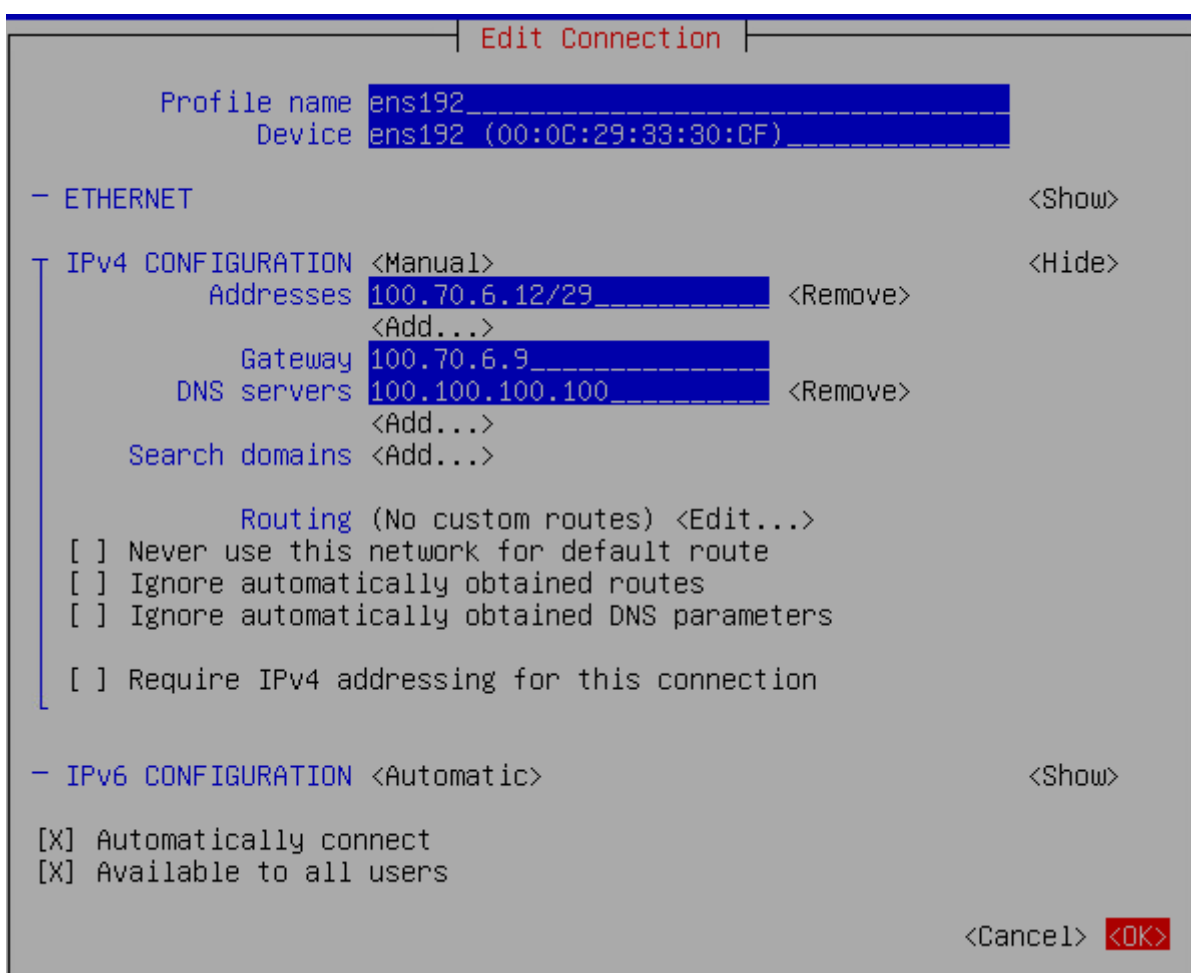
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



ClientEU

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.5.55/28

Шлюз 100.70.5.49

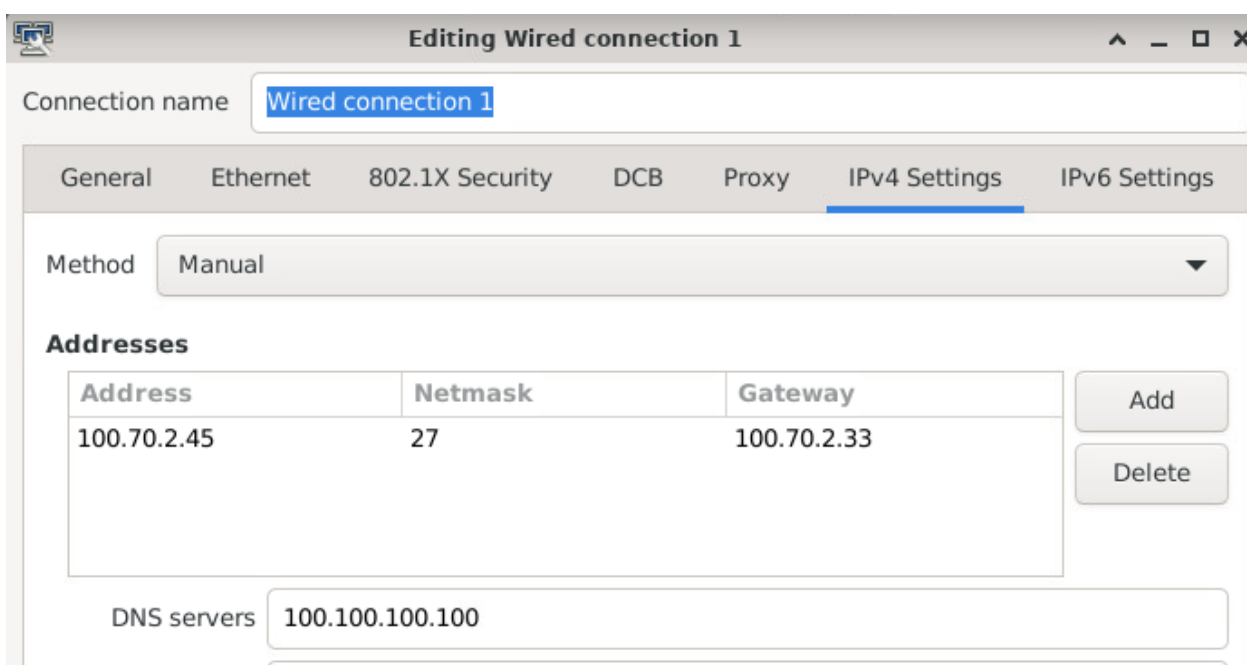
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
100.70.2.45	27	100.70.2.33

Add Delete

DNS servers: 100.100.100.100

VPNClient

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.6.13/29

Шлюз 100.70.6.9

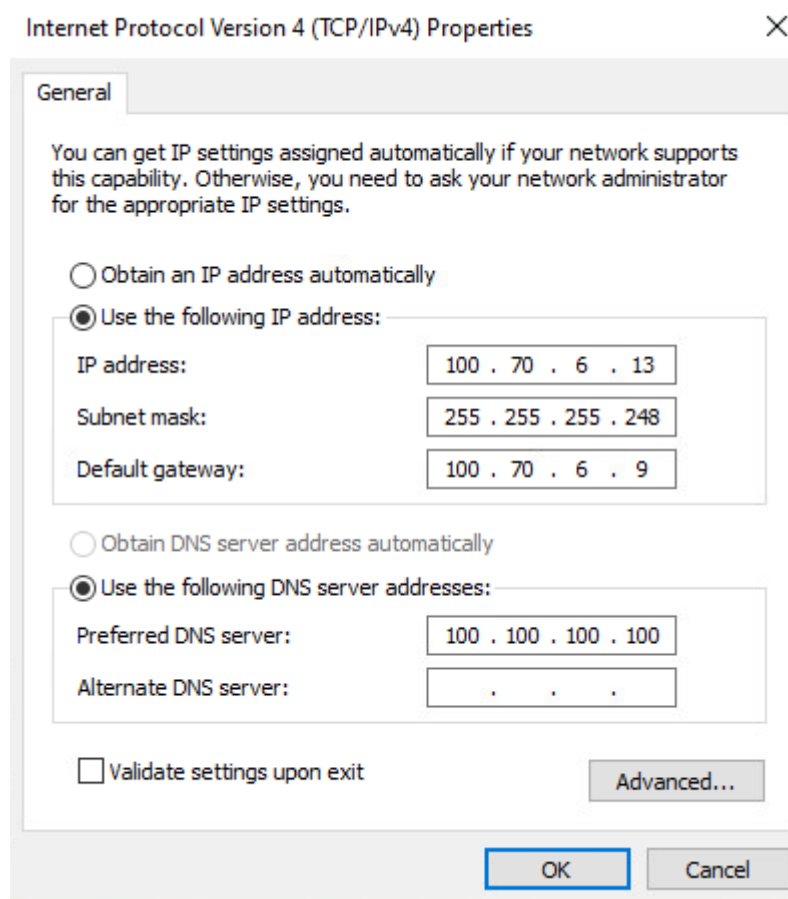
DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru



FW-AMS

Выбираем опцию 2 (Set interface IP address)

```
Available interfaces:

1 - LAN (vmx0 - static, track6)
2 - WAN (vmx1 - dhcp, dhcp6)

Enter the number of the interface to configure: 2

Configure IPv4 address WAN interface via DHCP? [Y/n] n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 100.70.4.18

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 28

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 100.70.4.17
```

```
Do you want to use it as the default IPv4 gateway? [Y/n] y

Do you want to use the gateway as the IPv4 name server, too? [Y/n] n
Enter the IPv4 name server or press <ENTER> for none:
> 100.100.100.100

Configure IPv6 address WAN interface via DHCP6? [Y/n] n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Restore web GUI access defaults? [y/N] y
```

Получаем

```
*** OPNsense.localdomain: OPNsense 23.1 ***

LAN (vmx0)      -> v4: 192.168.1.1/24
WAN (vmx1)      -> v4: 100.70.4.18/28

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █
```

Выбираем опцию 8 (Shell)

Вводим команду pfctl -d

Выходим из shell командой exit

```
root@OPNsense:~ # pfctl -d
pf disabled
root@OPNsense:~ # exit█
```

Проверка

С ClientSPB

через терминал

ping 100.70.4.18

через браузер

<http://100.70.4.18>

Открываем внешний доступ на FW-MSK

На ClientSPB заходим через браузер 100.70.4.18

Переходим Firewall – Rules – WAN и создаем разрешающее правило

Сохраняем, НО не применяем

Переходим Interfaces – WAN и убираем галочку Block private networks

Сохраняем и применяем настройки

Ждем применения правил. ДОСТУП ПОЛУЧЕН!

Через браузер настраиваем FW-MSK

LAN – 192.168.10.1/24

DMZ – 192.168.20.1/24

Службы – DHCPv4 – LAN убираем галочку Включен

Обновляем OPNSense (через консоль выбираем опцию 12)

Система – Программное обеспечение – Плагины – os-frr (устанавливаем)

Настраиваем OSPF

Маршрутизация – OSPF

Маршрутизация: OSPF

Общие настройки	Сети	Интерфейсы	Списки префиксов	Карты маршрутизации
-----------------	------	------------	------------------	---------------------

расширенный режим

Включен	<input checked="" type="checkbox"/>
CARP demote	<input type="checkbox"/>
Пассивные интерфейсы	DMZ, WAN
	Очистить все
Перераспределение маршрута	Ничего не выбрано
	Очистить все
Redistribution Map	отсутствует
Advertise Default Gateway	<input checked="" type="checkbox"/>
Always Advertise Default Gateway	<input type="checkbox"/>
Advertise Default Gateway Metric	<input type="text"/>

Маршрутизация: OSPF

Общие настройки

Сети

Интерфейсы

Списки префиксов

Карты маршрутизации

Включен

Адрес сети

Маска

Area



192.168.10.0

24

0.0.0.0



192.168.20.0

24

0.0.0.0

«

<


1

>

»

Маршрутизация – Общие настройки

Маршрутизация: Общие настройки

 расширенный режим

 Включен



 Enable CARP Failover



 Enable SNMP AgentX Support



 Enable logging



 Log Level

Уведомления

Сохранить

R0

configure

show interfaces

edit interfaces ethernet eth0

set address 192.168.10.2/24

set description FW

exit

edit interfaces ethernet eth1

set address 192.168.11.1/24

set description PC

exit

edit interfaces ethernet eth2

set address 192.168.12.1/24

set description PC

exit

commit

save

show interfaces

set protocols ospf area 0 network 192.168.10.0/24

set protocols ospf area 0 network 192.168.11.0/24

set protocols ospf area 0 network 192.168.12.0/24

set protocols ospf interface eth1 passive

set protocols ospf interface eth2 passive

commit

save

show protocols ospf

Проверка

exit

show ip ospf route

```
vyos@vyos:~$  
vyos@vyos:~$ show ip ospf route  
vtysh_pam: Failed in account validation: Success(0)=====  
ting table =====  
N    192.168.10.0/24      [1] area: 0.0.0.0  
                        directly attached to eth0  
N    192.168.11.0/24      [1] area: 0.0.0.0  
                        directly attached to eth1  
N    192.168.12.0/24      [1] area: 0.0.0.0  
                        directly attached to eth2  
  
===== OSPF router routing table =====  
R    192.168.20.1         [1] area: 0.0.0.0, ASBR  
                        via 192.168.10.1, eth0  
  
===== OSPF external routing table =====  
N E2 0.0.0.0/0           [1/10] tag: 0  
                        via 192.168.10.1, eth0  
  
vyos@vyos:~$
```

SRV1-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.12.2/24

Шлюз 192.168.12.1

DNS 192.168.10.1 (адрес интерфейса LAN на FW-MSK)

Проверка:

ping 192.168.12.1

Edit Connection

Profile nameens192

Deviceens192 (00:0C:29:8F:09:AB)

ETHERNET

IPv4 CONFIGURATION

<Manual>

Addresses192.168.12.2/24

<Add...>

Gateway192.168.12.1

DNS servers192.168.10.1

<Add...>

Search domains<Add...>

Routing (No custom routes) <Edit...>

[] Never use this network for default route

[] Ignore automatically obtained routes

[] Ignore automatically obtained DNS parameters

[] Require IPv4 addressing for this connection

IPv6 CONFIGURATION

<Automatic>

<Show>

<Hide>

<Remove>

<Remove>

<Edit...>

<Show>

[X] Automatically connect

[X] Available to all users

<Cancel>

<OK>

SRV2-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.12.3/24

Шлюз 192.168.12.1

DNS 192.168.10.1 (адрес интерфейса LAN на FW-MSK)

Проверка:

ping 192.168.12.1

Edit Connection

Profile name ens192
Device ens192 (00:0C:29:92:46:BD)

— ETHERNET <Show>

— IPv4 CONFIGURATION <Manual> <Hide>

Addresses 192.168.12.3/24 <Remove>
<Add...>

Gateway 192.168.12.1
DNS servers 192.168.10.1 <Remove>
<Add...>

Search domains <Add...>

Routing (No custom routes) <Edit...>

[] Never use this network for default route
[] Ignore automatically obtained routes
[] Ignore automatically obtained DNS parameters
[] Require IPv4 addressing for this connection

— IPv6 CONFIGURATION <Automatic> <Show>

[X] Automatically connect
[X] Available to all users

<Cancel> <OK>

Чтобы клиенты сети LAN-MSK и SRV-MSK имели доступ в интернет, необходимо на FW-MSK подправить правила Межсетевого экрана на интерфейсе LAN, настроить NAT и включить перенаправление DNS запросов

1) Правила Межсетевого экрана на интерфейсе LAN

Межсетевой экран: Правила: LAN

Выберите категорию

Изменения успешно применены.

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание
Automatically generated rules								
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	*	Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	*	*	*	*	*	*	Default allow LAN IPv6 to any rule
<input checked="" type="checkbox"/>	разрешение	<input checked="" type="checkbox"/>	блокирование	<input checked="" type="checkbox"/>	отклонение	<input checked="" type="checkbox"/>	журналирование	→ входящий
<input checked="" type="checkbox"/>	разрешение (отключено)	<input checked="" type="checkbox"/>	блокирование (отключено)	<input checked="" type="checkbox"/>	отклонение (отключено)	<input checked="" type="checkbox"/>	журналирование (отключено)	← исходящий

2) Правила NAT

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Перенаправление портов

One-to-One

Исходящий

NPTv6

Правила

Ограничитель трафика

Настройки

Межсетевой экран: NAT: Исходящий

Режим:

☐ Автоматическое создание правил исходящего NAT (нельзя использовать созданные вручную правила)

☒ Ручное создание правил исходящего NAT (правила не будут созданы автоматически)

☐ Смешанное создание правил исходящего NAT (автоматически созданные правила применяются после созданных вручную правил)

☐ Отключить создание правил исходящего NAT (исходящий NAT отключен)

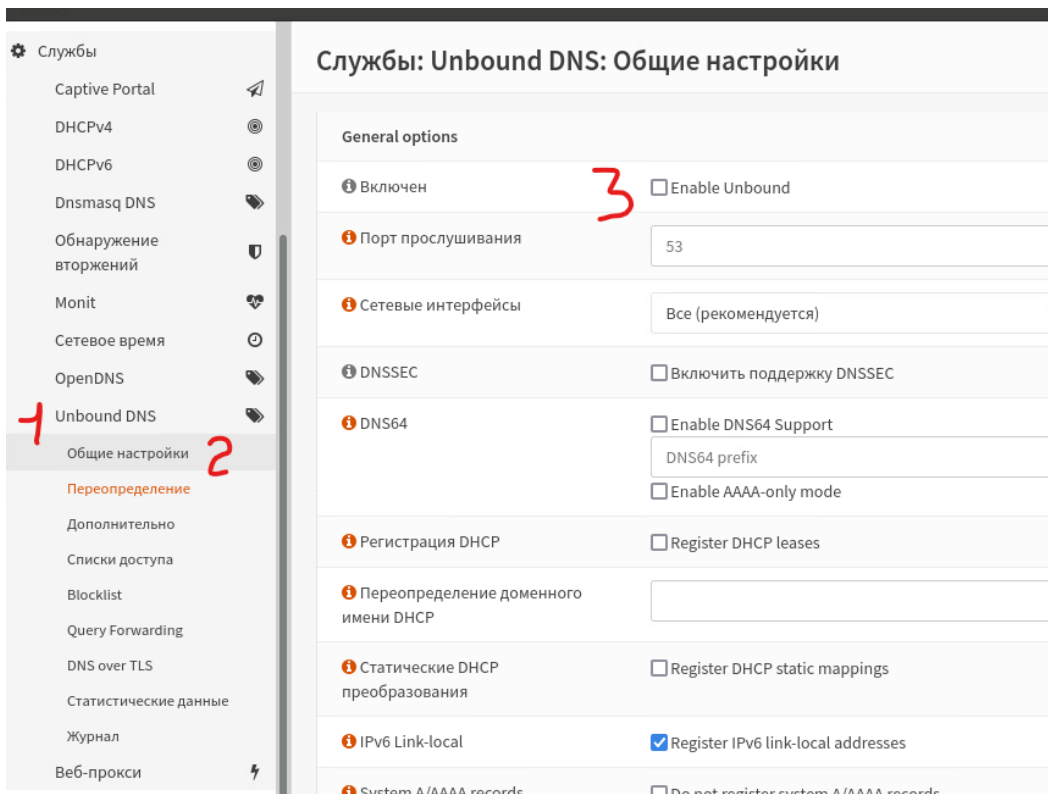
Сохранить

Manual rules

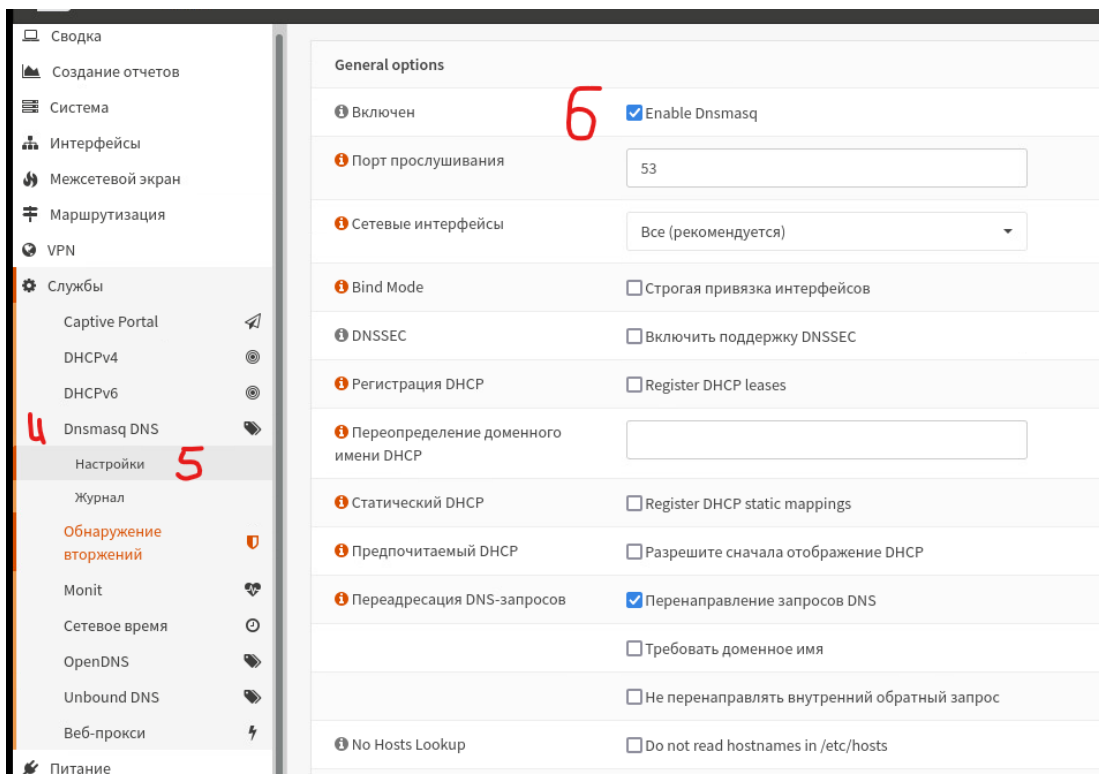
Выберите категорию

	Интерфейс	Источник	Порт источника	Назначение	Порт назначения	Адрес NAT	NAT порт	Статический порт	Описание
<input checked="" type="checkbox"/>	WAN	любой	*	*	*	Адрес интерфейса	*	НЕТ	
<input checked="" type="checkbox"/>	Правило включено								
<input type="checkbox"/>	Правило отключено								

3) Перенаправление DNS запросов



Сохранить настройки



Сохранить настройки

Проверка

На SRV-MSK1 – ping 8.8.8.8 и ping ya.ru

На SRV-MSK2 – ping 8.8.8.8 и ping ya.ru

APP-MSK

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.20.2/24

Шлюз 192.168.20.1

DNS 192.168.20.1 (адрес интерфейса DMZ на FW-MSK)

Profile name ens192
Device ens192 (00:0C:29:51:08:D1)

— ETHERNET <Show>

IPv4 CONFIGURATION <Manual> <Hide>

Addresses 192.168.20.2/24 <Remove>
<Add...>

Gateway 192.168.20.1

DNS servers 192.168.20.1 <Remove>
<Add...>

Search domains <Add...>

Routing (No custom routes) <Edit...>

[] Never use this network for default route
[] Ignore automatically obtained routes
[] Ignore automatically obtained DNS parameters
[] Require IPv4 addressing for this connection

— IPv6 CONFIGURATION <Automatic> <Show>

[X] Automatically connect
[X] Available to all users

<Cancel> <OK>

Чтобы клиенты сети DMZ-MSK имели доступ в интернет и не имели доступ к сети LAN-MSK и SRV-MSK, необходимо на FW-MSK создать правило Межсетевого экрана на интерфейсе DMZ

Межсетевой экран: Правила: DMZ

Выберите категорию

Inspect

Изменения успешно применены.

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?	
	Automatically generated rules 23								
	IPv4 *	DMZ сеть	*	192.168.10.0/24	*	*	*		
	IPv4 *	DMZ сеть	*	192.168.11.0/24	*	*	*		
	IPv4 *	DMZ сеть	*	192.168.12.0/24	*	*	*		
	IPv4 *	*	*	*	*	*	*		
▶ разрешение	✗ блокирование	⚠ отклонение	ℹ журналирование	→ входящий	⚡ первое совпадение				
▶ разрешение (отключено)	✗ блокирование (отключено)	⚠ отклонение (отключено)	ℹ журналирование (отключено)	← исходящий	⚡ последнее совпадение				

Проверка:

ping 192.168.12.2 – доступа нет

ping 192.168.12.3 – доступа нет

ping 192.168.11.1 – доступа нет

ping 100.100.100.100 – доступ есть

ping ya.ru – доступ есть

Настройка DHCP

SRV1-MSK

nano /etc/apt/sources.list

```
# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

#deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

deb http://deb.debian.org/debian/ bullseye main contrib
deb-src http://deb.debian.org/debian/ bullseye main contrib

# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bullseye-security main contrib
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bullseye-security main contrib

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://deb.debian.org/debian/ bullseye-updates main contrib
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib
~
```

apt update

apt list --upgradable

apt install isc-dhcp-server

nano /etc/default/isc-dhcp-server

```
# On what interfaces should the daemon listen
# Separate multiple interfaces with spaces
INTERFACESv4="ens192"
#INTERFACESv6=""
~
```

reboot

nano /etc/dhcp/dhcpd.conf

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "msk.jun39.wsr";
option domain-name-servers 192.168.10.1;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 doesn't
# have support for DDNS.)
ddns-update-style none;
```

```
# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.
```

```
subnet 192.168.12.0 netmask 255.255.255.0 {
}
```

```
# This is a very basic subnet declaration.
```

```
subnet 192.168.11.0 netmask 255.255.255.0 {
    range 192.168.11.20 192.168.11.240;
    option routers 192.168.11.1;
    option ntp-servers 192.168.10.1;
}
```

```
# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.
```

systemctl restart isc-dhcp-server

systemctl status isc-dhcp-server

```
root@SRV1-MSK:~# systemctl restart isc-dhcp-server
root@SRV1-MSK:~# systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Tue 2023-03-28 06:19:59 EDT; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 664 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 1129)
   Memory: 4.5M
      CPU: 43ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─679 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens192

Mar 28 06:19:57 SRV1-MSK systemd[1]: Starting LSB: DHCP server...
Mar 28 06:19:57 SRV1-MSK /usr/sbin/dhcpd: [664] Listening on TPv4 server only.
```

R0

configure

set service dhcp-relay interface eth1

set service dhcp-relay interface eth2

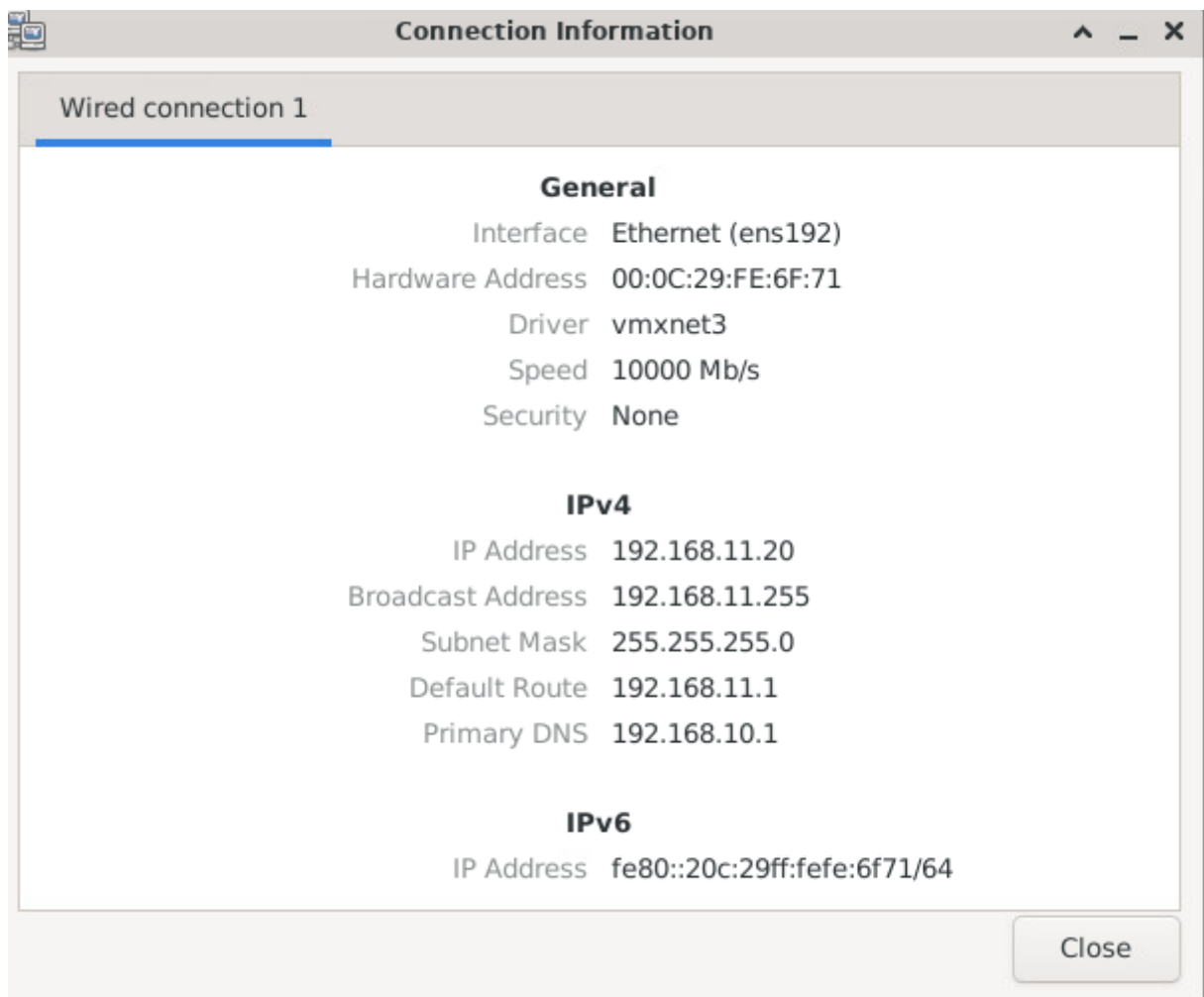
set service dhcp-relay server 192.168.12.2

commit

save

PC-MSK

Пробуем получить адрес по DHCP



ping ya.ru

Настройка имени, доменного имени, часового пояса

FW-MSK

Изменения успешно применены.

Система	
Имя хоста	FW-MSK
Домен	msk.jun39.wsr
Часовой пояс	Europe/Moscow
Язык	Русский
Тема	opnsense

SRV1-MSK

```
hostnamectl set-hostname SRV1-MSK.msk.jun39.wsr
```

```
timedatectl set-timezone Europe/Moscow
```

SRV2-MSK

```
hostnamectl set-hostname SRV2-MSK.msk.jun39.wsr
```

```
timedatectl set-timezone Europe/Moscow
```

PC-MSK

```
hostnamectl set-hostname PC-MSK.msk.jun39.wsr
```

```
timedatectl set-timezone Europe/Moscow
```

R0

```
configure
```

```
set system host-name R0-MSK
```

```
set system domain-name msk.jun39.wsr
```

```
set system time-zone Europe/Moscow
```

```
set service ntp server 192.168.10.1  
commit  
save
```

APP-MSK

```
hostnamectl set-hostname APP-MSK.msk.jun39.wsr  
timedatectl set-timezone Europe/Moscow
```

Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией

FW-MSK

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Маршрутизация

VPN

Службы

Captive Portal

DHCPv4

DHCPv6

Dnsmasq DNS

Настройки

Журнал

Обнаружение вторжений

Monit

Local DNS entry TTL

1

Сохранить

Переопределение хоста

Хост	Домен	IP-адрес	Описание
app-msk	msk.jun39.wsr	192.168.20.2	
fw-msk	msk.jun39.wsr	192.168.10.1	
r0-msk	msk.jun39.wsr	192.168.10.2	
srv1-msk	msk.jun39.wsr	192.168.12.2	
srv2-msk	msk.jun39.wsr	192.168.12.3	

Записи в этом разделе переопределяют отдельные результаты из Используйте их для изменения результатов DNS или добавления записей заказного DNS.

Настройка синхронизации времени

FW-MSK

Службы: Сетевое время: Общие настройки

Конфигурация NTP-сервера

Серверы времени	Сеть	Предпочитать
-	100.101.102.103	<input checked="" type="checkbox"/>
-	1.opnsense.pool.ntp.org	<input type="checkbox"/>
-	2.opnsense.pool.ntp.org	<input type="checkbox"/>
-	3.opnsense.pool.ntp.org	<input type="checkbox"/>
+		

Client mode ☐ Quit NTP server immediately after time synchronisation

Интерфейсы Все (рекомендуется)

Автономный режим 12

SRV1-MSK

apt install chrony

nano /etc/chrony/chrony.conf

```
# Use Debian vendor zone.  
pool 192.168.10.1 iburst
```

systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

```

root@SRV1-MSK:~# chronyc tracking
Reference ID      : COA80A01 (FW-MSK)
Stratum          : 4
Ref time (UTC)   : Wed Mar 29 04:55:46 2023
System time      : 0.000006323 seconds fast of NTP time
Last offset      : +0.000013660 seconds
RMS offset       : 0.000013660 seconds
Frequency        : 7.824 ppm slow
Residual freq    : -10.862 ppm
Skew             : 49.836 ppm
Root delay       : 0.014233872 seconds
Root dispersion  : 0.942363620 seconds
Update interval  : 2.0 seconds
Leap status      : Normal
root@SRV1-MSK:~#

```

SRV2-MSK

nano /etc/apt/sources.list

```

# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bulls
eye contrib main

#deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullse
ye contrib main

deb http://deb.debian.org/debian/ bullseye main contrib
deb-src http://deb.debian.org/debian/ bullseye main contrib

# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bullseye-security main contrib
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bullseye-security main contrib

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://deb.debian.org/debian/ bullseye-updates main contrib
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib
~

```

apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf

```

# Use Debian vendor zone.
pool 192.168.10.1 iburst

```

systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

```
root@SRV2-MSK:~# systemctl restart chrony
root@SRV2-MSK:~# chronyc tracking
Reference ID      : COA80A01 (FW-MSK)
Stratum          : 4
Ref time (UTC)   : Wed Mar 29 05:07:53 2023
System time      : 0.000012959 seconds fast of NTP time
Last offset      : +0.000014464 seconds
RMS offset       : 0.000014464 seconds
Frequency        : 16.941 ppm slow
Residual freq    : +9.212 ppm
Skew             : 1000000.000 ppm
Root delay       : 0.013393632 seconds
Root dispersion  : 0.985263109 seconds
Update interval  : 2.0 seconds
Leap status      : Normal
```

APP-MSK

nano /etc/apt/sources.list

```
# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

#deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

deb http://deb.debian.org/debian/ bullseye main contrib
deb-src http://deb.debian.org/debian/ bullseye main contrib

# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bullseye-security main contrib
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bullseye-security main contrib

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://deb.debian.org/debian/ bullseye-updates main contrib
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib
~
```

apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf

```
# Use Debian vendor zone.  
pool 192.168.20.1 iburst
```

systemctl restart chrony

systemctl status chrony

Проверка

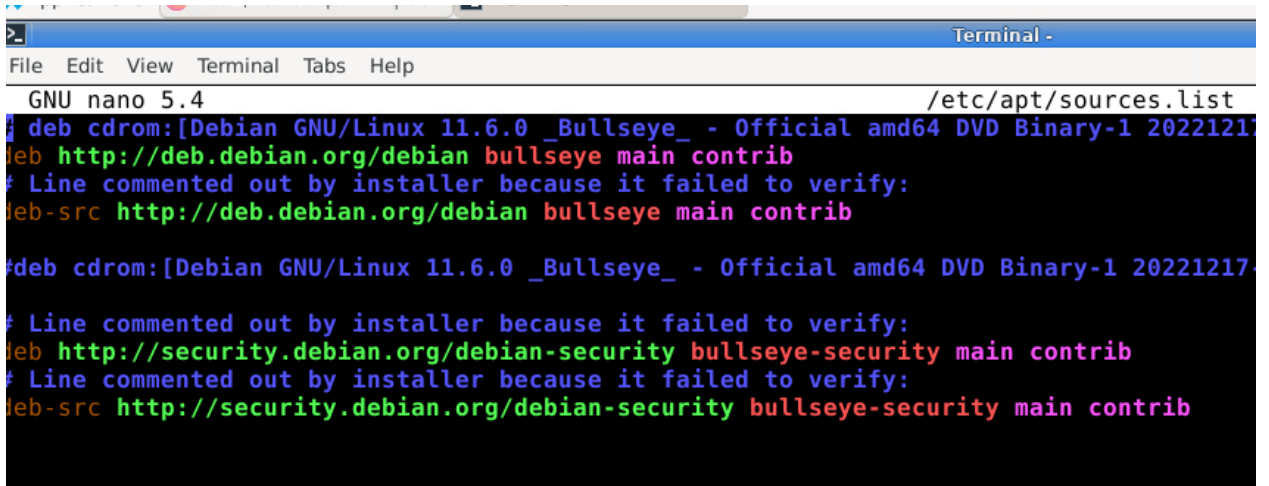
chronyc tracking

```
root@APP-MSK:~# chronyc tracking  
Reference ID      : C0A81401 (192.168.20.1)  
Stratum          : 4  
Ref time (UTC)   : Wed Mar 29 07:02:21 2023  
System time      : 0.000000020 seconds slow of NTP time  
Last offset      : +0.000177241 seconds  
RMS offset       : 0.000928455 seconds  
Frequency        : 15.687 ppm slow  
Residual freq    : +0.051 ppm  
Skew             : 4.683 ppm  
Root delay       : 0.014183724 seconds  
Root dispersion  : 0.017890921 seconds  
Update interval  : 64.5 seconds  
Leap status      : Normal  
root@APP-MSK:~#
```

ClientSPB

timedatectl set-timezone Europe/Moscow

nano /etc/apt/sources.list



```
GNU nano 5.4 /etc/apt/sources.list
# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217]
deb http://deb.debian.org/debian bullseye main contrib
# Line commented out by installer because it failed to verify:
deb-src http://deb.debian.org/debian bullseye main contrib

# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217]
# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bullseye-security main contrib
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bullseye-security main contrib
```

apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf



```
# Use Debian vendor zone.
pool 100.101.102.103 iburst
```

systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

```
root@ClientSPB:~# chronyc tracking
Reference ID      : 64656667 (100.101.102.103)
Stratum          : 3
Ref time (UTC)   : Wed Mar 29 07:33:27 2023
System time      : 0.000000021 seconds fast of NTP time
Last offset      : -0.000019771 seconds
RMS offset       : 0.000019771 seconds
Frequency        : 15.627 ppm slow
Residual freq    : -13.187 ppm
Skew             : 0.270 ppm
Root delay       : 0.013304343 seconds
Root dispersion  : 0.002518897 seconds
Update interval  : 2.0 seconds
Leap status      : Normal
root@ClientSPB:~# █
```

```
root@ClientSPB:~# timedatectl
          Local time: Wed 2023-03-29 10:36:57 MSK
          Universal time: Wed 2023-03-29 07:36:57 UTC
             RTC time: Wed 2023-03-29 07:36:57
          Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@ClientSPB:~# █
```

VDS

timedatectl set-timezone Asia/Yekaterinburg

nano /etc/apt/sources.list

```
# deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

#deb cdrom:[Debian GNU/Linux 11.6.0 _Bullseye_ - Official amd64 DVD Binary-1 20221217-10:40]/ bullseye contrib main

deb http://deb.debian.org/debian/ bullseye main contrib
deb-src http://deb.debian.org/debian/ bullseye main contrib

# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bullseye-security main contrib
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bullseye-security main contrib

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://deb.debian.org/debian/ bullseye-updates main contrib
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib
~
```

apt update

apt list --upgradable

apt install chrony

nano /etc/chrony/chrony.conf

```
# Use Debian vendor zone.
pool 100.101.102.103 iburst
```

systemctl restart chrony

systemctl status chrony

Проверка

chronyc tracking

timedatectl

```
root@VDS:~# systemctl restart chrony
root@VDS:~# chronyc tracking
Reference ID      : 64656667 (100.101.102.103)
Stratum          : 3
Ref time (UTC)   : Wed Mar 29 07:45:41 2023
System time      : 0.000000463 seconds fast of NTP time
Last offset      : -0.000876777 seconds
RMS offset       : 0.000876777 seconds
Frequency        : 23.354 ppm slow
Residual freq    : -1.616 ppm
Skew             : 1000000.000 ppm
Root delay       : 0.013332226 seconds
Root dispersion  : 1.731365204 seconds
Update interval  : 0.0 seconds
Leap status      : Normal
root@VDS:~# _
```

```
root@VDS:~# timedatectl
root@VDS:~# timedatectl
          Local time: Wed 2023-03-29 12:46:16 +05
          Universal time: Wed 2023-03-29 07:46:16 UTC
             RTC time: Wed 2023-03-29 07:46:17
          Time zone: Asia/Yekaterinburg (+05, +0500)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@VDS:~#
```


Сетевое обнаружение по протоколу LLDP

SRV1-MSK, SRV2-MSK, APP-MSK

apt install lldpd

Проверка

lldctl

FW-MSK

Создание отчетов	os-igmp-proxy	1.5_2	22.7KiB	OPNsense	IGMP-Proxy Service	0 +
Система 1	os-intrusion-detection-content-et-open	1.0.1	1.53KiB	OPNsense	IDS Proofpoint ET open ruleset complementary subset for ET Pro Telemetry edition	0 +
Доступ	os-intrusion-detection-content-et-pro	1.0.2_1	5.71KiB	OPNsense	IDS Proofpoint ET Pro ruleset (needs a valid subscription)	0 +
Конфигурация	os-intrusion-detection-content-pt-open	1.0_1	789B	OPNsense	IDS PT Research ruleset (only for non-commercial use)	0 +
2 Программное обеспечение	os-intrusion-detection-content-snort-vrt	1.1_1	12.7KiB	OPNsense	IDS Snort VRT ruleset (needs registration or subscription)	0 +
Статус	os-iperf	1.0_1	24.6KiB	OPNsense	Connection speed tester	0 +
Настройки	os-lcdproc-sdeclcd	1.1_1	941B	OPNsense	LCDProc for SDEC LCD devices	0 +
Журнал изменений	os-lldpd	1.1_2	16.5KiB	OPNsense	LLDP allows you to know exactly on which port is a server	0 + 4
Обновления	os-maltrail	1.10	45.6KiB	OPNsense	Malicious traffic detection system	0 +
Плагины	os-mdns-repeater	1.1	17.9KiB	OPNsense	Proxy multicast DNS between networks	0 +
Пакеты 3	os-munin-node	1.1_1	14.8KiB	OPNsense	Munin monitoring agent	0 +
Средство создания отчетов	os-net-snmp	1.5_2	27.3KiB	OPNsense	Net-SNMP is a daemon for the SNMP protocol	0 +
Журнал						

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Маршрутизация

VPN

1 Службы

Captive Portal

DHCPv4

DHCPv6

Dnsmasq DNS

Обнаружение вторжений

2 LLDPd

Monit

Сетевое время

Службы: LLDPd

Общие настройкиСоседние

Enable LLDP Daemon

Enable CDP

Enable FDP

Enable EDP

Enable SONMP

Interface Configuration

Сохранить 3

R0

configure

set service lldp

commit

save

Проверка

show lldp neighbors

Удаленный доступ по SSH

R0

configure

set service ssh port 22

commit

save

Проверка

С PC-MSK подключаемся по SSH

ssh vyos@r0-msk

```
File Edit View Terminal Tabs Help
root@PC-MSK:~# ssh vyos@r0-msk
The authenticity of host 'r0-msk (192.168.10.2)' can't be established.
ECDSA key fingerprint is SHA256:RN0apHwwC75FoJEFsQ1NaZey1zmJvmo5bX9PYbz5LU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'r0-msk,192.168.10.2' (ECDSA) to the list of known hosts.
vyos@r0-msk's password:
Welcome to VyOS!

Check out project news at https://blog.vyos.io
and feel free to report bugs at https://vyos.dev

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright
vyos@R0:~$
vyos@R0:~$
```

VDS

```
apt install ssh
```

```
systemctl status sshd
```

```
su user
```

```
mkdir /home/user/.ssh
```

На PC-MSK заходим под пользователем user с паролем P@ssw0rd

```
ssh-keygen
```

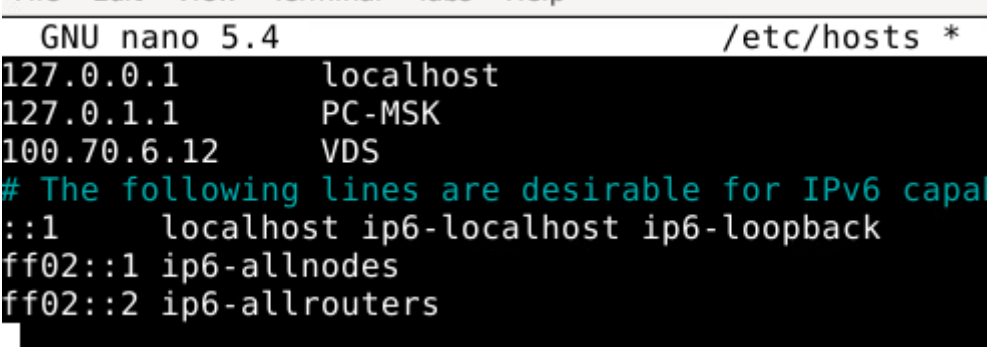
```
cd /home/user/.ssh/
```

```
ls -l
```

```
scp id_rsa.pub user@100.70.6.12:/home/user/.ssh/authorized_keys
```

```
su root
```

```
nano /etc/hosts
```



```
GNU nano 5.4 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    PC-MSK
100.70.6.12   VDS
# The following lines are desirable for IPv6 capability
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

```
exit
```

Проверка

```
ssh user@VDS
```

```
user@PC-MSK:~/.ssh$ ssh user@VDS
The authenticity of host 'vds (100.70.6.12)' can't be established.
ECDSA key fingerprint is SHA256:T3dB4et1CEbBHPtoifcuQ7JsarkETy9WKq02f0lmgM0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'vds' (ECDSA) to the list of known hosts.
Linux VDS 5.10.0-20-amd64 #1 SMP Debian 5.10.158-2 (2022-12-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 29 13:36:53 2023 from 100.70.4.18
user@VDS:~$
```

Офис AMS

На FW-AMS

WAN – 100.70.3.45/26, шлюз 100.70.3.1, DNS 100.100.100.100

DMZ – 192.168.2.1/24

Обновляем OPNSense (через консоль выбираем опцию 12)

Система – Программное обеспечение – Плагины – os-ftp и lldp (устанавливаем)

Настраиваем Межсетевой экран

1) на интерфейсе LAN

Межсетевой экран: Правила: LAN Выберите категорию

Изменения успешно применены.

<input type="checkbox"/>	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
<input type="checkbox"/>								<i>Automatically generated rules</i>
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	*	Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	*	*	*	*	*	*	Default allow LAN IPv6 to any rule
<input type="checkbox"/>	разрешение	✗ блокирование	✗ отклонение	📘 журналирование	→ входящий			
<input type="checkbox"/>	разрешение (отключено)	✗ блокирование (отключено)	✗ отклонение (отключено)	📘 журналирование (отключено)	← исходящий			

2) на интерфейсе DMZ

Межсетевой экран: Правила: DMZ Выберите категорию

Изменения успешно применены.

<input type="checkbox"/>	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
<input type="checkbox"/>	✗ IPv4 *	DMZ сеть	*	LAN сеть	*	*	*	
<input type="checkbox"/>	→ IPv4 *	*	*	*	*	*	*	
<input type="checkbox"/>	разрешение	✗ блокирование	✗ отклонение	📘 журналирование	→ входящий			
<input type="checkbox"/>	разрешение (отключено)	✗ блокирование (отключено)	✗ отклонение (отключено)	📘 журналирование (отключено)	← исходящий			

📅 Active/Inactive Schedule (click to view/edit)

📄 Псевдоним (нажмите для просмотра/редактирования)

3) на интерфейсе WAN

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Правила

Floating

LAN

Loopback

WAN

Межсетевой экран: Правила: WAN

Выберите категорию

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
								Automatically generated rules
	IPv4 *	*	*	*	*	*	*	
разрешение	блокирование	отклонение	журналирование	→ входящий				
разрешение (отключено)	блокирование (отключено)	отклонение (отключено)	журналирование (отключено)	← исходящий				
Active/Inactive Schedule (click to view/edit)								

4) Правила NAT

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Перенадресация портов

One-to-One

Исходящий

NPTv6

Правила

Ограничитель трафика

Настройки

Межсетевой экран: NAT: Исходящий

Режим:

Автоматическое создание правил исходящего NAT (нельзя использовать созданные вручную правила)

Смешанное создание правил исходящего NAT (автоматически созданные правила применяются после созданных вручную правил)

Ручное создание правил исходящего NAT (правила не будут созданы автоматически)

Отключить создание правил исходящего NAT (исходящий NAT отключен)

Сохранить

Manual rules

Выберите категорию

	Интерфейс	Источник	Порт источника	Назначение	Порт назначения	Адрес NAT	NAT порт	Статический порт	Описание
	WAN	любой	*	*	*	Адрес интерфейса	*	НЕТ	
	Правило включено								
	Правило отключено								

Настраиваем перенаправление DNS запросов

Службы

- Captive Portal
- DHCPv4
- DHCPv6
- Dnsmasq DNS
- Обнаружение вторжений
- Monit
- Сетевое время
- OpenDNS
- 1 Unbound DNS 2
 - Общие настройки
 - Переопределение
 - Дополнительно
 - Списки доступа
 - Blocklist
 - Query Forwarding
 - DNS over TLS
 - Статистические данные
 - Журнал
 - Веб-прокси

Службы: Unbound DNS: Общие настройки

General options

- 3 Включен ☐ Enable Unbound
- Порт прослушивания 53
- Сетевые интерфейсы Все (рекомендуется)
- DNSSEC ☐ Включить поддержку DNSSEC
- DNS64 ☐ Enable DNS64 Support
DNS64 prefix
☐ Enable AAAA-only mode
- Регистрация DHCP ☐ Register DHCP leases
- Переопределение доменного имени DHCP
- Статические DHCP преобразования ☐ Register DHCP static mappings
- IPv6 Link-local ☒ Register IPv6 link-local addresses
- System A/AAAA records ☐ Do not register system A/AAAA records

Сохранить настройки

Сводка

- Создание отчетов
- Система
- Интерфейсы
- Межсетевой экран
- Маршрутизация
- VPN
- Службы
 - Captive Portal
 - DHCPv4
 - DHCPv6
 - 4 Dnsmasq DNS 5
 - Настройки
 - Журнал
 - Обнаружение вторжений
 - Monit
 - Сетевое время
 - OpenDNS
 - Unbound DNS
 - Веб-прокси
- Питание

Службы: Dnsmasq DNS: Общие настройки

General options

- 6 Включен ☒ Enable Dnsmasq
- Порт прослушивания 53
- Сетевые интерфейсы Все (рекомендуется)
- Bind Mode ☐ Строгая привязка интерфейсов
- DNSSEC ☐ Включить поддержку DNSSEC
- Регистрация DHCP ☐ Register DHCP leases
- Переопределение доменного имени DHCP
- Статический DHCP ☐ Register DHCP static mappings
- Предпочитаемый DHCP ☐ Разрешите сначала отображение DHCP
- Переадресация DNS-запросов ☒ Перенаправление запросов DNS
- ☐ Требовать доменное имя
- ☐ Не перенаправлять внутренний обратный запрос
- No Hosts Lookup ☐ Do not read hostnames in /etc/hosts

Проверка

На PC-AMS – ping 8.8.8.8 и ping ya.ru

Настройка DHCP на интерфейсе LAN

Система

Интерфейсы

Межсетевой экран

VPN

Службы

Captive Portal

DHCPv4

[DMZ]

[LAN]

[WAN]

Ретрансляция

Аренда адресов

Журнал

DHCPv6

Dnsmasq DNS

Обнаружение

Ignore Client UUIDs

Подсеть

192.168.1.0

Маска подсети

255.255.255.0

Доступный диапазон

192.168.1.1 - 192.168.1.254

Диапазон

от

192.168.1.20

до

192.168.1.240

Дополнительные пулы

Начало пула

Конец пула

Описание

WINS-серверы

DNS-серверы

192.168.1.1

адресам

NTP-серверы

192.168.1.1

Настройка имени, доменного имени, часового пояса

Программное обеспечение

Шлюзы

Высокий уровень доступности

Маршруты

Настройки

Администрирование

Планировщик задач Cron

Общие настройки

Журналирование

Logging / targets

Прочее

Система

Имя хоста

FW-AMS

Домен

ams.jun39.wsr

Часовой пояс

Europe/Amsterdam

Язык

Русский

Тема

opnsense

Настройка синхронизации времени

Интерфейсы
Межсетевой экран
Маршрутизация
VPN
Службы 1

Captive Portal
DHCPv4
DHCPv6
Dnsmasq DNS
Обнаружение вторжений
Monit
Сетевое время 2
Общие настройки 3
GPS-приемник
PPS
Статус
Журнал

Службы: Сетевое время: Общие настройки

Конфигурация NTP-сервера

Серверы времени

	Сеть	Предпочитать
-	100.101.102.103 ✓	<input checked="" type="checkbox"/>
-	1.opnsense.pool.ntp.org	<input type="checkbox"/>
-	2.opnsense.pool.ntp.org	<input type="checkbox"/>
-	3.opnsense.pool.ntp.org	<input type="checkbox"/>
+		

Client mode ☐ Quit NTP server immediately after time synchronisation

Интерфейсы Все (рекомендуется)

Автономный режим 12

Настройка LLDP

Сводка
Создание отчетов
Система
Интерфейсы
Межсетевой экран
Маршрутизация
VPN
Службы 1

Captive Portal
DHCPv4
DHCPv6
Dnsmasq DNS
Обнаружение вторжений
LLDPd 2
Monit
Сетевое время

Службы: LLDPd

Общие настройки | Соседние

Enable LLDP Daemon ☒ ✓

Enable CDP ☒ ✓

Enable FDP ☐

Enable EDP ☐

Enable SONMP ☐

Interface Configuration

Сохранить 3

Настройка доступа по именам

Переопределение хоста		
Хост	Домен	IP-адрес
app-ams	ams.jun39.wsr	192.168.2.3
dmz-ams	ams.jun39.wsr	192.168.2.2
fw-ams	ams.jun39.wsr	192.168.1.1
Записи в этом разделе переопределяют отдельные результаты из Используйте их для изменения р		

DMZ-AMS

1) Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.2.2/24

Шлюз 192.168.2.1

DNS 192.168.2.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname DMZ-AMS.ams.jun39.wsr
```

```
timedatectl set-timezone Europe/Amsterdam
```

```
apt install chrony
```

```
nano /etc/chrony/chrony.conf
```

```
# Use Debian vendor zone.  
pool 192.168.2.1 iburst
```

```
systemctl restart chrony
```

```
systemctl status chrony
```

Проверка

```
chronyc tracking
```

```
timedatectl
```

3) Устанавливаем LLDP

```
apt install lldpd
```

Проверка

```
lldpdctl
```

APP-AMS

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.2.3/24

Шлюз 192.168.2.1

DNS 192.168.2.1

Проверка:

ping 192.168.2.2 и ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname APP-AMS.ams.jun39.wsr
```

```
timedatectl set-timezone Europe/Amsterdam
```

```
apt install chrony
```

```
nano /etc/chrony/chrony.conf
```

```
# Use Debian vendor zone.  
pool 192.168.2.1 iburst
```

```
systemctl restart chrony
```

```
systemctl status chrony
```

Проверка

```
chronyc tracking
```

```
timedatectl
```

3) Устанавливаем LLDP

```
apt install lldpd
```

Проверка

```
lldpctl
```


PC-AMS

Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname PC-AMS.ams.jun39.wsr
```

```
timedatectl set-timezone Europe/Amsterdam
```

```
apt install chrony
```

Проверка

```
timedatectl
```

```
File Edit View Terminal Tabs Help
root@PC-AMS:~# timedatectl
          Local time: Wed 2023-03-29 13:05:45 CEST
          Universal time: Wed 2023-03-29 11:05:45 UTC
          RTC time: Wed 2023-03-29 11:05:45
          Time zone: Europe/Amsterdam (CEST, +0200)
System clock synchronized: yes
          NTP service: active
          RTC in local TZ: no
root@PC-AMS:~#
```

```
chronyc sources
```

```
root@PC-AMS:~# chronyc sources
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^- 195.218.227.166           2    6   177   33  -1119us[-1119us] +/-  71ms
^+ yggnode.cf                2    6   177   32  -1800us[-1800us] +/-  13ms
^- ns5.vlz.su                2    6   177   33  +2407us[+2407us] +/-  67ms
^* stratum2-1.ntp.mow01.ru.> 2    6   177   33  -5074us[-6776us] +/-  14ms
^+ FW-AMS                    3    6   177   32   +12ms[  +12ms] +/-  30ms
root@PC-AMS:~#
```

Офис ИКТ

На FW-ИКТ

WAN – 100.70.7.99/25, шлюз 100.70.7.1, DNS 100.100.100.100

DMZ – 192.168.4.1/24

Обновляем OPNSense (через консоль выбираем опцию 12)

Система – Программное обеспечение – Плагины – os-ftp и lldp (устанавливаем)

Меняем настройки DHCP сервера

Службы 1

Captive Portal

DHCPv4 2

[DMZ]

[LAN] 3

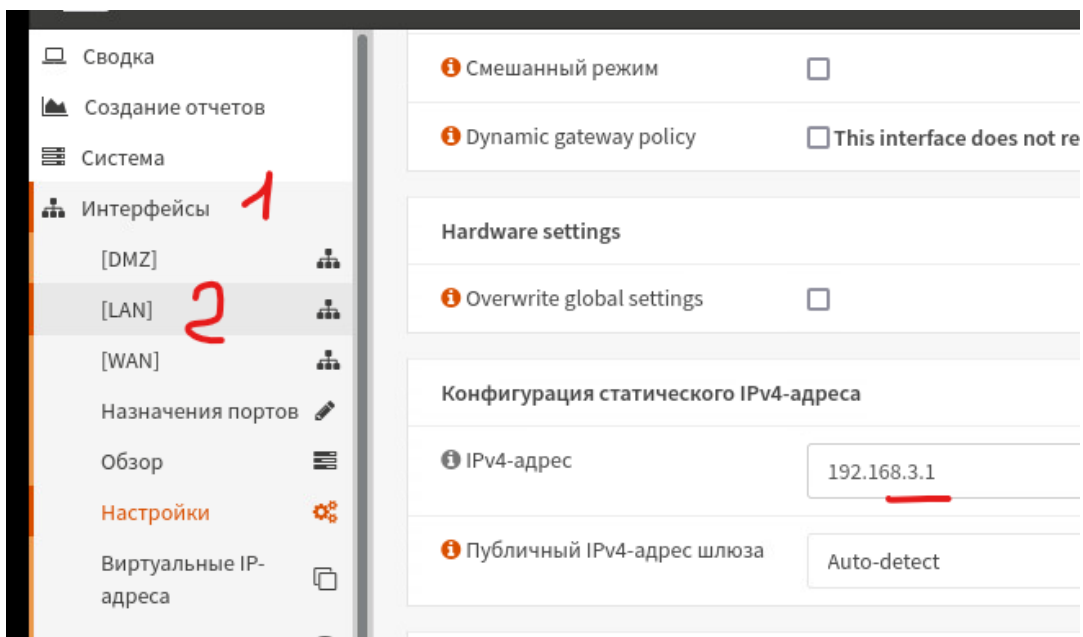
[WAN]

Ретрансляция

Подсеть	192.168.3.0		
Маска подсети	255.255.255.0		
Доступный диапазон	192.168.3.1 - 192.168.3.254		
Диапазон	от	до	
	192.168.3.20	192.168.3.240	
Дополнительные пулы	Начало пула	Конец пула	Описание
WINS-серверы			
NTP-серверы	192.168.3.1		

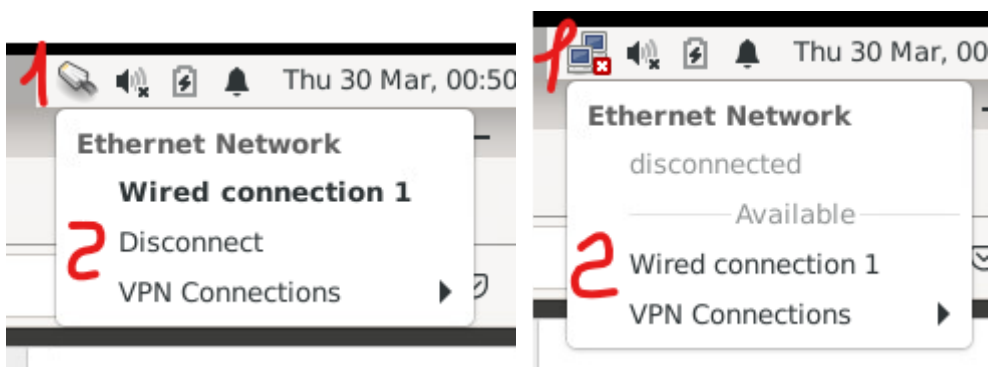
Сохраняем, но настройки НЕ ПРИМЕНЯЕМ

Меняем адрес на LAN

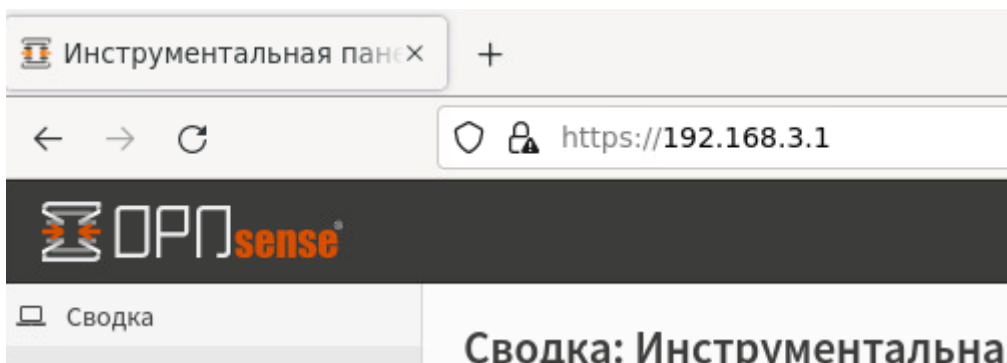


Сохраняем, применяем настройки. ТЕРЯЕТСЯ ДОСТУП!

На PC-ИКТ перезапускаем сетевой интерфейс



ПОЯВЛЯЕТСЯ ДОСТУП по новому адресу



Настраиваем Межсетевой экран

1) на интерфейсе LAN

Межсетевой экран: Правила: LAN

Выберите категорию

Изменения успешно применены.

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
Automatically generated rules								
	IPv4 *	*	*	*	*	*	*	Default allow LAN to any rule
	IPv6 *	*	*	*	*	*	*	Default allow LAN IPv6 to any rule
разрешение		блокирование		отклонение			журналирование	→ входящий
разрешение (отключено)		блокирование (отключено)		отклонение (отключено)			журналирование (отключено)	← исходящий

2) на интерфейсе DMZ

Межсетевой экран: Правила: DMZ

Выберите категорию

Изменения успешно применены.

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
	IPv4 *	DMZ сеть	*	LAN сеть	*	*	*	
	IPv4 *	*	*	*	*	*	*	
разрешение		блокирование		отклонение			журналирование	→ входящий
разрешение (отключено)		блокирование (отключено)		отклонение (отключено)			журналирование (отключено)	← исходящий

Active/Inactive Schedule (click to view/edit)

Псевдоним (нажмите для просмотра/редактирования)

3) на интерфейсе WAN

Межсетевой экран: Правила: WAN

Выберите категорию

	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание ?
Automatically generated rules								
	IPv4 *	*	*	*	*	*	*	
разрешение		блокирование		отклонение			журналирование	→ входящий
разрешение (отключено)		блокирование (отключено)		отклонение (отключено)			журналирование (отключено)	← исходящий

Active/Inactive Schedule (click to view/edit)

4) Правила NAT

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Перезадресация портов

One-to-One

Исходящий

НПТv6

Правила

Ограничитель трафика

Настройки

Межсетевой экран: NAT: Исходящий

Режим:

☐ Автоматическое создание правил исходящего NAT (нельзя использовать созданные вручную правила)

☐ Смешанное создание правил исходящего NAT (автоматически созданные правила применяются после созданных вручную правил)

☒ Ручное создание правил исходящего NAT (правила не будут созданы автоматически)

☐ Отключить создание правил исходящего NAT (исходящий NAT отключен)

Сохранить

Manual rules

Выберите категорию

<input type="checkbox"/>	Интерфейс	Источник	Порт источника	Назначение	Порт назначения	Адрес NAT	NAT порт	Статический порт	Описание
<input checked="" type="checkbox"/>	WAN	любой	*	*	*	Адрес интерфейса	*	НЕТ	
									Правило включено
									Правило отключено

Настраиваем перенаправление DNS запросов

Службы

Captive Portal

DHCPv4

DHCPv6

Dnsmasq DNS

Обнаружение вторжений

Monit

Сетевое время

OpenDNS

Unbound DNS

Общие настройки

Переопределение

Дополнительно

Списки доступа

Blocklist

Query Forwarding

DNS over TLS

Статистические данные

Журнал

Веб-прокси

Службы: Unbound DNS: Общие настройки

General options

☒ Включен 3 ☐ Enable Unbound

1 Порт прослушивания

1 Сетевые интерфейсы

1 DNSSEC ☐ Включить поддержку DNSSEC

1 DNS64 ☐ Enable DNS64 Support

☐ Enable AAAA-only mode

1 Регистрация DHCP ☐ Register DHCP leases

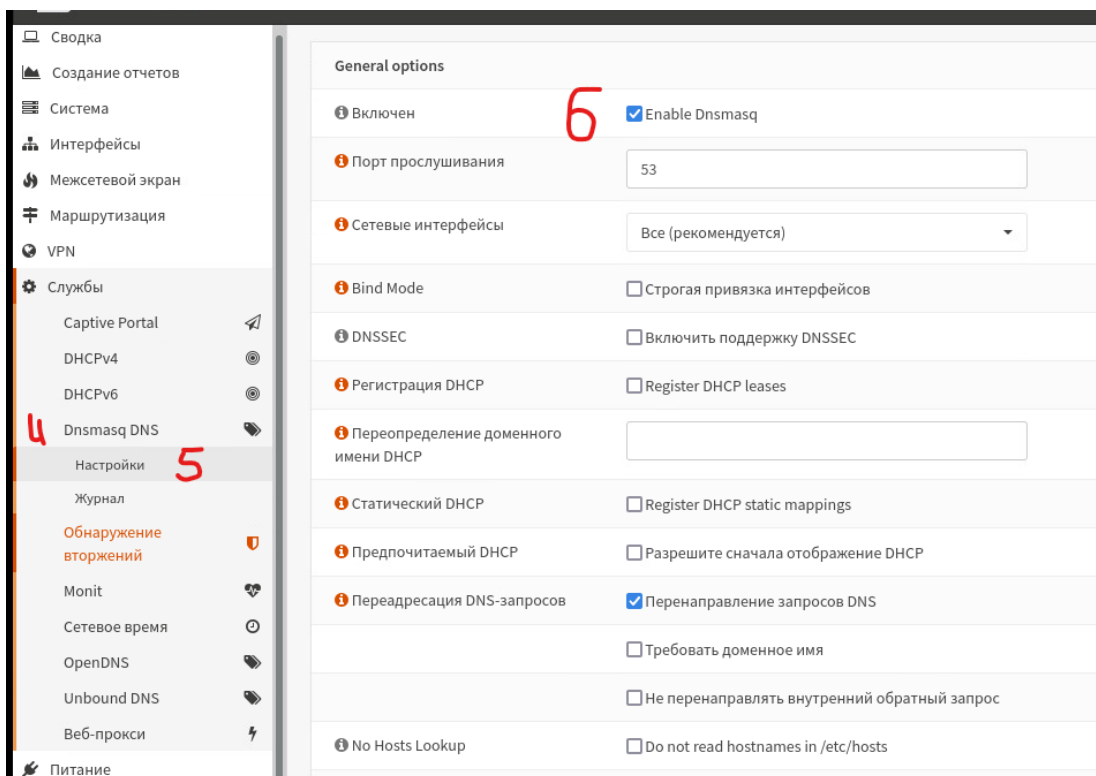
1 Переопределение доменного имени DHCP

1 Статические DHCP преобразования ☐ Register DHCP static mappings

1 IPv6 Link-local ☒ Register IPv6 link-local addresses

1 System A/AAAA records ☐ Do not register system A/AAAA records

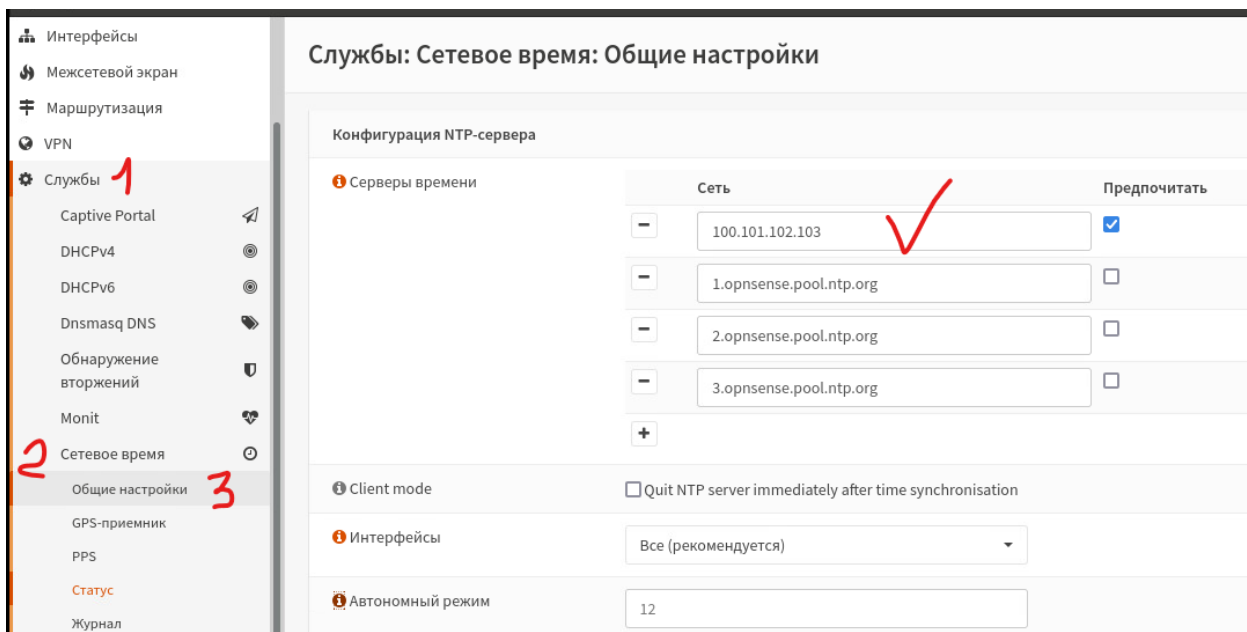
Сохранить настройки



Проверка

На PC-ИКТ – ping 8.8.8.8 и ping ya.ru

Настройка синхронизации времени



Настройка LLDP

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Маршрутизация

VPN

Службы

Captive Portal

DHCPv4

DHCPv6

Dnsmasq DNS

Обнаружение вторжений

LLDPd

Monit

Сетевое время

Службы: LLDPd

Общие настройкиСоседние

Enable LLDP Daemon

Enable CDP

Enable FDP

Enable EDP

Enable SONMP






Interface Configuration

Сохранить

Настройка доступа по именам

Переопределение хоста		
Хост	Домен	IP-адрес
app-ikt	ikt.jun39.wsr	192.168.4.3
fw-ikt	ikt.jun39.wsr	192.168.3.1
srv1-ikt	ikt.jun39.wsr	192.168.3.2
www	jun39.wsr	192.168.4.3

Общие настройки

Система	
 Имя хоста	<input type="text" value="FW-IKT"/>
 Домен	<input type="text" value="ikt.jun39.wsr"/>
 Часовой пояс	<input type="text" value="Asia/Irkutsk"/>
 Язык	<input type="text" value="Русский"/>
 Тема	<input type="text" value="opnsense"/>

PC-IKT

Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname PC-IKT.ikt.jun39.wsr
```

```
timedatectl set-timezone Asia/Irkutsk
```

```
apt install chrony
```

Проверка

```
timedatectl
```

```
root@PC-IKT:~# timedatectl
Local time: Thu 2023-03-30 13:41:52 +08
Universal time: Thu 2023-03-30 05:41:52 UTC
RTC time: Thu 2023-03-30 05:41:52
Time zone: Asia/Irkutsk (+08, +0800)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
root@PC-IKT:~#
```

chronyc sources

```
root@PC-IKT:~# chronyc sources
MS Name/IP address          Stratum Poll Reach L
=====
^- 213.234.203.30            2      6    17
^- ns1.ooonet.ru             2      6    17
^- nsa.lds.net.ua            2      6    17
^+ roswell.systems           2      6    17
^* FW-IKT                    3      6    17
root@PC-IKT:~#
```

Аренда адресов

SRV1-IKT

1) Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.3.2/24

Шлюз 192.168.3.1

DNS 192.168.3.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname SRV1-IKT.ikt.jun39.wsr
```

```
timedatectl set-timezone Asia/Irkutsk
```

```
apt install chrony
```

```
nano /etc/chrony/chrony.conf
```

```
# Use Debian vendor zone.  
pool 192.168.3.1 iburst
```

```
systemctl restart chrony
```

```
systemctl status chrony
```

Проверка

```
chronyc tracking
```

```
timedatectl
```

3) Устанавливаем LLDP

```
apt install lldpd
```

Проверка

```
lldpdctl
```


APP-ИКТ

Назначаем адрес согласно принятой схеме IP-адресации:

Адрес 192.168.4.3/24

Шлюз 192.168.4.1

DNS 192.168.4.1

Проверка:

ping 8.8.8.8 и ping ya.ru

2) Устанавливаем имя, время и часовой пояс

```
hostnamectl set-hostname APP-ИКТ.икт.юн39.вср
```

```
timedatectl set-timezone Asia/Irkutsk
```

```
apt install chrony
```

```
nano /etc/chrony/chrony.conf
```

```
# Use Debian vendor zone.  
pool 192.168.4.1 iburst
```

```
systemctl restart chrony
```

```
systemctl status chrony
```

Проверка

```
chronyc tracking
```

```
timedatectl
```

3) Устанавливаем LLDP

```
apt install lldpd
```

Проверка

```
lldpctl
```

ClientVV

Назначаем адрес согласно схеме IP-адресации:

Адрес 100.70.8.78/28

Шлюз 100.70.8.65

DNS 100.100.100.100

Проверка:

ping 100.101.102.103

ping 8.8.8.8

ping ya.ru

Создание пользователя

SRV1-ITK

apt install sudo

adduser admin

```
root@SRV1-IKT:~# adduser admin
Adding user `admin' ...
Adding new group `admin' (1001) ...
Adding new user `admin' (1001) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@SRV1-IKT:~#
```

usermod -aG sudo admin

Проверка

groups admin

```
root@SRV1-IKT:~# groups admin
admin : admin sudo
root@SRV1-IKT:~# _
```

Настройка NFS сервера

SRV1-IKT

```
apt install nfs-kernel-server
```

```
mkdir -p /opt/nfs/rw
```

```
mkdir -p /opt/nfs/ro
```

```
chmod a+w /opt/nfs/rw
```

```
chmod a+w /opt/nfs/ro
```

```
touch /opt/nfs/rw/testRW.txt
```

```
touch /opt/nfs/ro/testRO.txt
```

```
chown -R admin:admin /opt/nfs
```

```
nano /etc/exports
```

```
/opt/nfs/rw 192.168.3.0/24(rw,sync)
```

```
/opt/nfs/ro 192.168.3.0/24(ro,sync)
```

```
systemctl restart nfs-server
```

Проверка

```
showmount -e 192.168.3.2
```

```
root@SRV1-IKT: ~#  
root@SRV1-IKT:~# showmount -e 192.168.3.2  
Export list for 192.168.3.2:  
/opt/nfs/ro 192.168.3.0/24  
/opt/nfs/rw 192.168.3.0/24  
root@SRV1-IKT:~#
```

Настройка NFS клиента

PC-IKT

```
apt install nfs-common
```

```
mkdir -p /home/user/Desktop/nfs_rw
```

```
mkdir -p /home/user/Desktop/nfs_ro
```

```
nano /etc/fstab
```

```
192.168.3.2:/opt/nfs/rw/ /home/user/Desktop/nfs_rw nfs defaults 0 0
```

```
192.168.3.2:/opt/nfs/ro/ /home/user/Desktop/nfs_ro nfs defaults 0 0
```

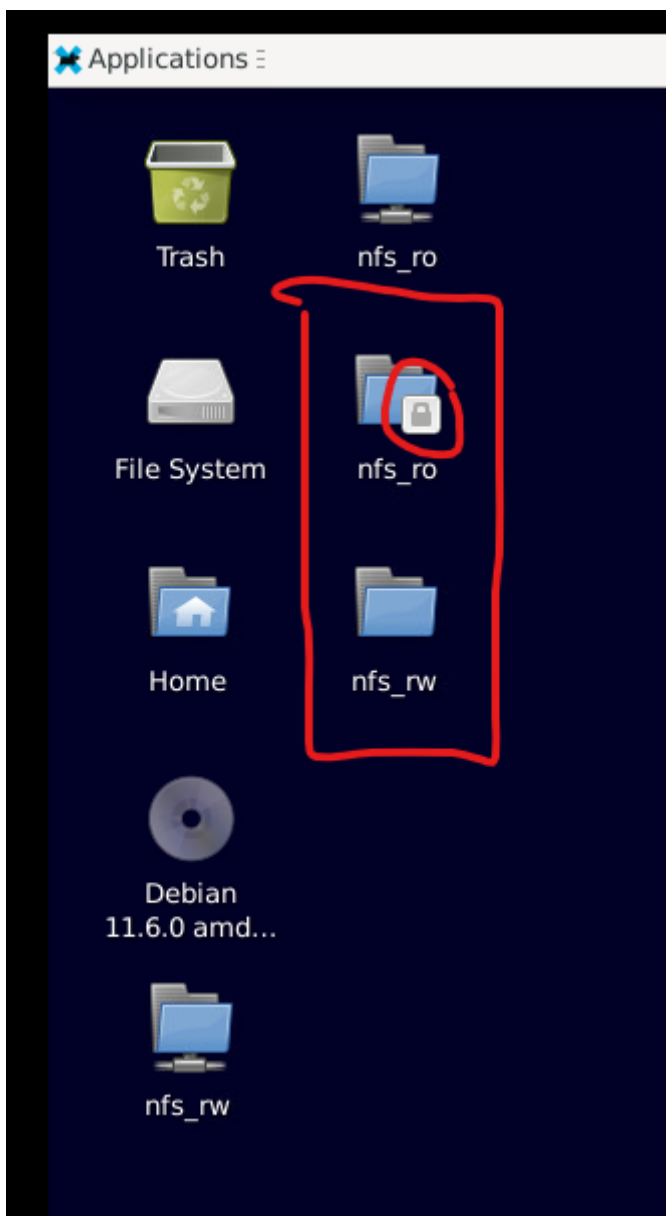
```
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=db92be75-00a5-4abf-b8da-9a07fbed1315 / ext4 errors=remount
# swap was on /dev/sda5 during installation
UUID=e81357f3-7f3e-4b99-83a7-5716945a740b none swap sw
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0
192.168.3.2:/opt/nfs/rw/ /home/user/Desktop/nfs_rw nfs defaults 0 0
192.168.3.2:/opt/nfs/ro/ /home/user/Desktop/nfs_ro nfs defaults 0 0
```

```
mount -a
```

```
df -h
```

```
root@PC-IKT:~# mount -a
root@PC-IKT:~# df -h
Filesystem              Size  Used Avail Use% Mounted on
udev                    465M   0    465M   0% /dev
tmpfs                    98M   1.1M   97M    2% /run
/dev/sda1                15G   3.4G   11G   25% /
tmpfs                   489M   0    489M   0% /dev/shm
tmpfs                    5.0M   0    5.0M   0% /run/lock
tmpfs                    98M   44K    98M   1% /run/user/0
192.168.3.2:/opt/nfs/rw  15G   1.2G   13G    9% /home/user/Desktop/nfs_rw
192.168.3.2:/opt/nfs/ro  15G   1.2G   13G    9% /home/user/Desktop/nfs_ro
root@PC-IKT:~#
```

Заходим на PC-IKT под пользователем user с паролем P@ssw0rd



WEB сервер на APP-*

APP-AMS

```
apt install nginx
```

```
touch /var/www/html/index.html
```

```
nano /var/www/html/index.html
```

Welcome to Minecraft server mc.jun39.wsr site in European region

```
systemctl restart nginx
```

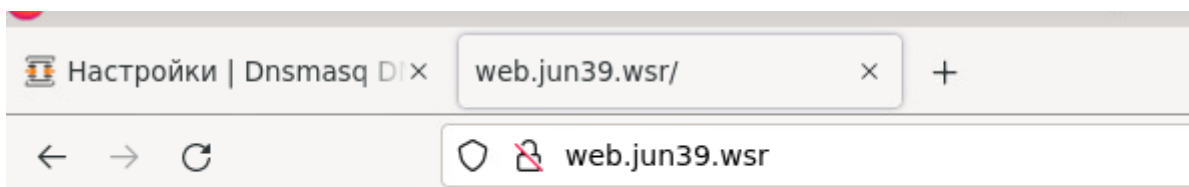
На FW-AMS

Переопределение хоста		
Хост	Домен	IP-адрес
app-ams	ams.jun39.wsr	192.168.2.3
dmz-ams	ams.jun39.wsr	192.168.2.2
fw-ams	ams.jun39.wsr	192.168.1.1
web	jun39.wsr	192.168.2.3

На PC-AMS

Проверка

В браузере вводим `http://web.jun39.wsr`



Welcome to Minecraft server mc.jun39.wsr site in European region

APP-MSK

```
apt install nginx
```

```
touch /var/www/html/index.html
```

```
nano /var/www/html/index.html
```

Welcome to Minecraft server mc.jun39.wsr site in Central region

```
systemctl restart nginx
```

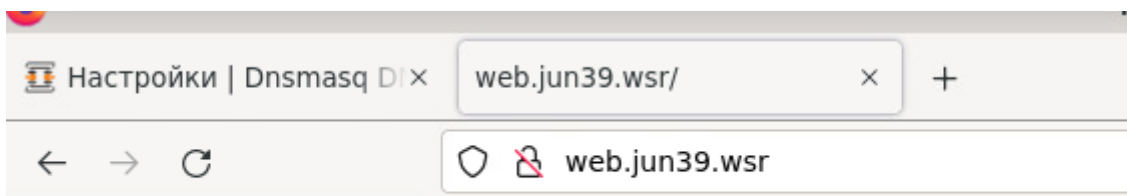
На FW-MSK

Переопределение хоста		
Хост	Домен	IP-адрес
app-msk	msk.jun39.wsr	192.168.20.2
fw-msk	msk.jun39.wsr	192.168.10.1
r0-msk	msk.jun39.wsr	192.168.10.2
srv1-msk	msk.jun39.wsr	192.168.12.2
srv2-msk	msk.jun39.wsr	192.168.12.3
web	jun39.wsr	192.168.20.2

На PC-MSK

Проверка

В браузере вводим <http://web.jun39.wsr>



Welcome to Minecraft server mc.jun39.wsr site in Central region

APP-IKT

```
apt install nginx
```

```
touch /var/www/html/index.html
```

```
nano /var/www/html/index.html
```

Welcome to Minecraft server mc.jun39.wsr site in Siberian region

```
systemctl restart nginx
```

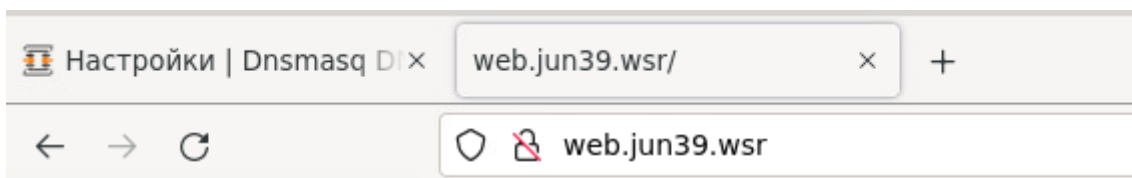
На FW-IKT

Переопределение хоста		
Хост	Домен	IP-адрес
app-ikt	ikt.jun39.wsr	192.168.4.3
fw-ikt	ikt.jun39.wsr	192.168.3.1
srv1-ikt	ikt.jun39.wsr	192.168.3.2
web	jun39.wsr	192.168.4.3

На PC-IKT

Проверка

В браузере вводим <http://web.jun39.wsr>



Welcome to Minecraft server mc.jun39.wsr site in Siberian region

Проброс порта для сайта на APP-*

FW-MSK (подключаемся через PC-MSK)

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Переадресация портов

One-to-One

Исходящий

NPTv6

Межсетевой экран: NAT: ПЕРЕАДРЕСАЦИЯ ПОРТОВ

Выберите категорию

Изменения успешно применены.

	Источник		Назначение		NAT				
	Интерфейс	Протокол	Адрес	Порты	Адрес	Порты	IP-адрес	Порты	Описание
<input type="checkbox"/>	LAN	TCP	*	*	LAN address	80	*	*	Правило антиблокировки
	Правило включено		Без перенаправления		Связанное правило				
	Правило отключено		Disabled no redirect		Disabled linked rule				
	Псевдоним (нажмите для просмотра/редактирования)								

Назначение

WAN адрес

Диапазон портов назначения

от:

к:

HTTP

HTTP

Перенаправление целевого IP-адреса

Одиночный хост или сеть

192.168.20.2

Целевой порт перенаправления

HTTP

Ассоциация правила фильтрации

Разрешение

5

Сохранить

Отменить

FW-AMS (подключаемся через PC-AMS)

Создание отчетов

Система

Интерфейсы

Межсетевой экран 1

Псевдонимы

Categories

Группы

2 NAT

3 Переадресация портов

One-to-One

Исходящий

NPTv6

Межсетевой экран: NAT: Переадресация портов

Выберите категорию

Изменения успешно применены.

	Источник		Назначение		NAT				
	Интерфейс	Протокол	Адрес	Порты	Адрес	Порты	IP-адрес	Порты	Описание
<input type="checkbox"/>	LAN	TCP	*	*	LAN address	80	*	*	Правило антиблокировки
<input checked="" type="checkbox"/>	Правило включено		!	Без перенаправления		→	Связанное правило		
<input type="checkbox"/>	Правило отключено		!	Disabled no redirect		→	Disabled linked rule		
Псевдоним (нажмите для просмотра/редактирования)									

Назначение

WAN адрес

Диапазон портов назначения

от: HTTP

к: HTTP

Перенаправление целевого IP-адреса

Одиночный хост или сеть

192.168.2.3

Целевой порт перенаправления

HTTP

Ассоциация правила фильтрации

Разрешение

5

Сохранить

Отменить

FW-ИКТ (подключаемся через РС-ИКТ)

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Псевдонимы

Categories

Группы

NAT

Переадресация портов

One-to-One

Исходящий

NPTv6

Межсетевой экран: NAT: Переадресация портов

Выберите категорию

Изменения успешно применены.

	Источник		Назначение		NAT				
<input type="checkbox"/>	Интерфейс	Протокол	Адрес	Порты	Адрес	Порты	IP-адрес	Порты	Описание
	LAN	TCP	*	*	LAN address	80	*	*	Правило антиблокировки
	Правило включено				Без перенаправления			Связанное правило	
	Правило отключено				Disabled no redirect			Disabled linked rule	
	Псевдоним (нажмите для просмотра/редактирования)								

Назначение	WAN адрес		✓
Диапазон портов назначения	от: HTTP	к: HTTP	
Перенаправление целевого IP-адреса	Одиночный хост или сеть	192.168.4.3	✓
Целевой порт перенаправления	HTTP		
Ассоциация правила фильтрации	Разрешение		✓
5			
Сохранить		Отменить	

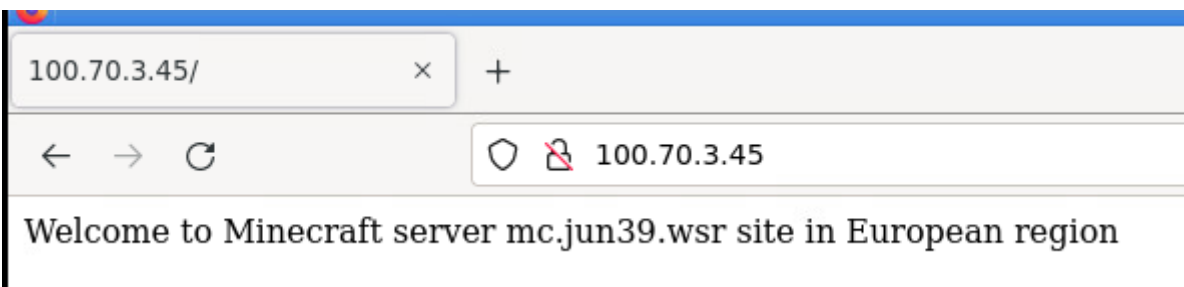
Проверка

На ClientSPB в браузере вводим

<http://100.70.3.45>

<http://100.70.4.18>

<http://100.70.7.99>



Настройка DNS сервера

VDS

apt install bind9

nano /etc/bind/named.conf

Закомментируем последнюю строку

```
// If you are just adding zones, please do that in  
  
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
#include "/etc/bind/named.conf.default-zones";  
~  
~
```

nano /etc/bind/named.conf.options

```
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and your clients  
    // to talk to, you may need to fix the firewall to allow  
    // ports to talk.  See http://www.kb.cert.org/vuls/id/20666  
  
    // If your ISP provided one or more IP addresses for  
    // nameservers, you probably want to use them.  Uncomment  
    // the following block, and change the placeholder to  
    // the all-0's placeholder.  
  
    forwarders {  
        100.100.100.100; ✓  
    };  
    forward first; ✓  
  
    //=====
```

// If BIND logs error messages about the
// you will need to update your keys.
//=====

```
    dnssec-validation no; ✓  
  
    listen-on { any; }; ✓  
    listen-on-v6 { none; }; ✓  
    allow-query { any; }; ✓  
};  
~
```

systemctl restart bind9

systemctl status bind9

```
cp /etc/bind/db.local /var/cache/bind/jun39.wsr
```

```
nano /var/cache/bind/jun39.wsr
```

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      jun39.wsr. root.jun39.wsr. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       jun39.wsr.
@         IN      A        100.70.6.12
```

```
cp /var/cache/bind/jun39.wsr /var/cache/bind/ams.jun39.wsr
```

```
nano /var/cache/bind/ams.jun39.wsr
```

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      jun39.wsr. root.jun39.wsr.
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative
;
@         IN      NS       jun39.wsr.
@         IN      A        100.70.6.12
web       IN      A        100.70.3.45 ✓
~
~
```

```
cp /var/cache/bind/jun39.wsr /var/cache/bind/msk.jun39.wsr
```

```
nano /var/cache/bind/msk.jun39.wsr
```

```

; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      jun39.wsr. root.jun39
                        2      ; Ser
                        604800   ; Ref
                        86400    ; Ret
                        2419200  ; Exp
                        604800 ) ; Neg

;
@         IN      NS       jun39.wsr.
@         IN      A        100.70.6.12
web       IN      A        100.70.4.18
~
~

```

cp /var/cache/bind/jun39.wsr /var/cache/bind/ikt.jun39.wsr
 nano /var/cache/bind/ikt.jun39.wsr

```

; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      jun39.wsr. root.jun39
                        2      ; Ser
                        604800   ; Ref
                        86400    ; Ret
                        2419200  ; Exp
                        604800 ) ; Neg

;
@         IN      NS       jun39.wsr.
@         IN      A        100.70.6.12
web       IN      A        100.70.7.99
~
~

```

chown bind:bind /var/cache/bind/*

ls -l /var/cache/bind/

```

root@VDS: ~# chown bind:bind /var/cache/bind/*
root@VDS:~# ls -l /var/cache/bind/
total 24
-rw-r--r-- 1 bind bind 279 Mar 30 13:13 ams.jun39.wsr
-rw-r--r-- 1 bind bind 279 Mar 30 13:14 ikt.jun39.wsr
-rw-r--r-- 1 bind bind 259 Mar 30 13:09 jun39.wsr
-rw-r--r-- 1 bind bind 221 Mar 30 13:03 managed-keys.bind
-rw-r--r-- 1 bind bind 1426 Mar 30 13:03 managed-keys.bind.jnl
-rw-r--r-- 1 bind bind 279 Mar 30 13:13 msk.jun39.wsr
root@VDS:~#

```



```
nano /etc/bind/named.conf.local
```

```
view "ams" {  
    match-clients { 100.70.2.45; };  
    zone "jun39.wsr" {  
        type master;  
        file "/var/cache/bind/ams.jun39.wsr";  
    };  
};
```

```
view "msk" {  
    match-clients { 100.70.5.55; };  
    zone "jun39.wsr" {  
        type master;  
        file "/var/cache/bind/msk.jun39.wsr";  
    };  
};
```

```
view "ikt" {  
    match-clients { 100.70.8.78; };  
    zone "jun39.wsr" {  
        type master;  
        file "/var/cache/bind/ikt.jun39.wsr";  
    };  
};
```

```
view "Default" {  
    match-clients { any; };  
    zone "jun39.wsr" {  
        type master;  
        file "/var/cache/bind/jun39.wsr";  
    };  
};
```

```
systemctl restart bind9
```

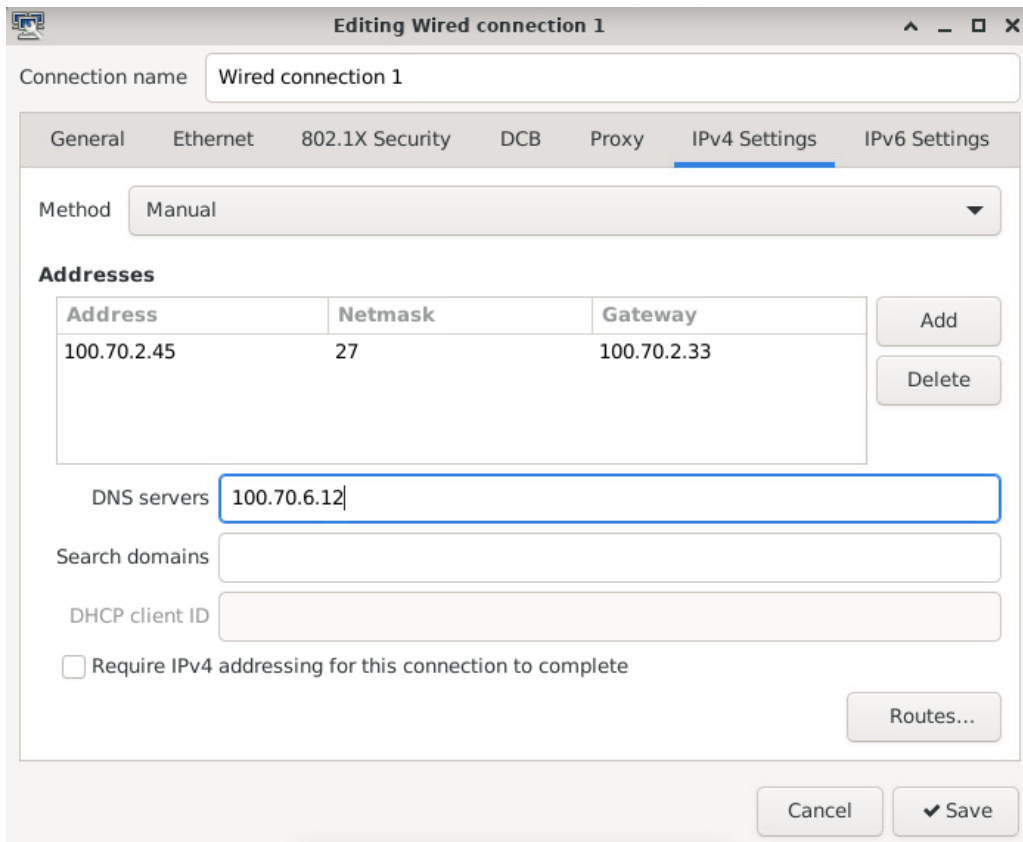
```
systemctl status bind9
```

```
root@VDS:~# systemctl status bind9
• named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset:
   Active: active (running) since Thu 2023-03-30 13:26:06 +05; 6s ago
     Docs: man:named(8)
  Main PID: 3856 (named)
    Tasks: 6 (limit: 2337)
   Memory: 29.8M
      CPU: 76ms
   CGroup: /system.slice/named.service
           └─3856 /usr/sbin/named -f -u bind

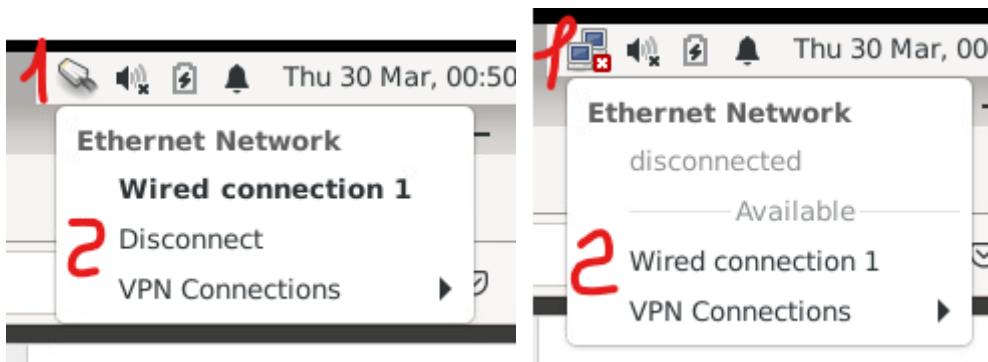
Mar 30 13:26:06 VDS named[3856]: managed-keys-zone/ams: loaded serial 0
Mar 30 13:26:06 VDS named[3856]: managed-keys-zone/msk: loaded serial 0
Mar 30 13:26:06 VDS named[3856]: managed-keys-zone/ikt: loaded serial 0
Mar 30 13:26:06 VDS named[3856]: managed-keys-zone/Default: loaded serial 0
Mar 30 13:26:06 VDS named[3856]: zone jun39.wsr/IN/ams: loaded serial 2
Mar 30 13:26:06 VDS named[3856]: zone jun39.wsr/IN/msk: loaded serial 2
Mar 30 13:26:06 VDS named[3856]: zone jun39.wsr/IN/ikt: loaded serial 2
Mar 30 13:26:06 VDS named[3856]: zone jun39.wsr/IN/Default: loaded serial 2
Mar 30 13:26:06 VDS named[3856]: all zones loaded
Mar 30 13:26:06 VDS named[3856]: running
root@VDS:~#
```

ClientEU

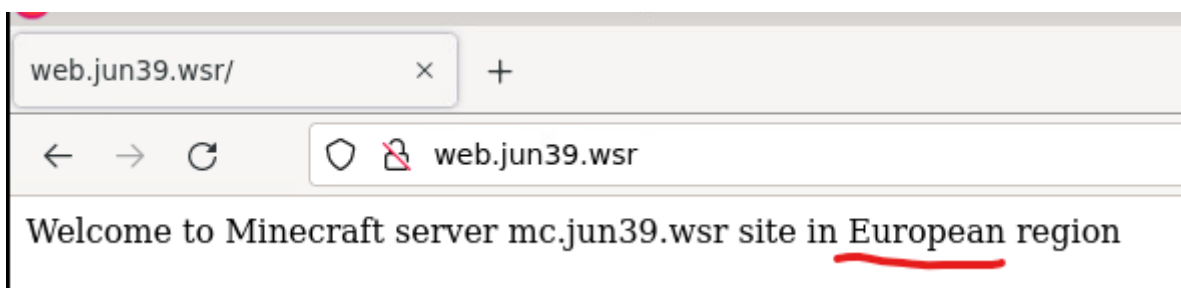
Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12



Перезапускаем сетевое подключение



В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-AMS

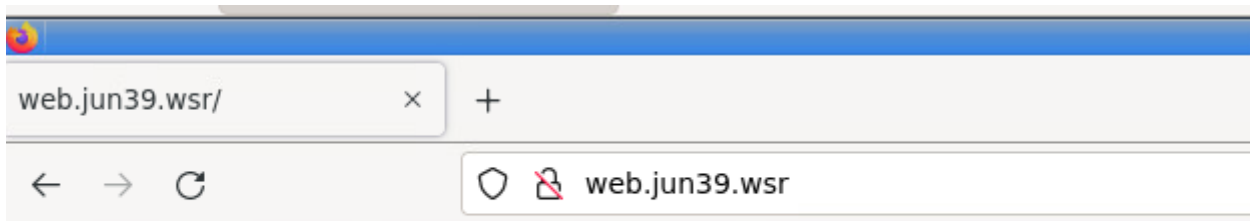


ClientSPB

Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12

Перезапускаем сетевое подключение

В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-MSK

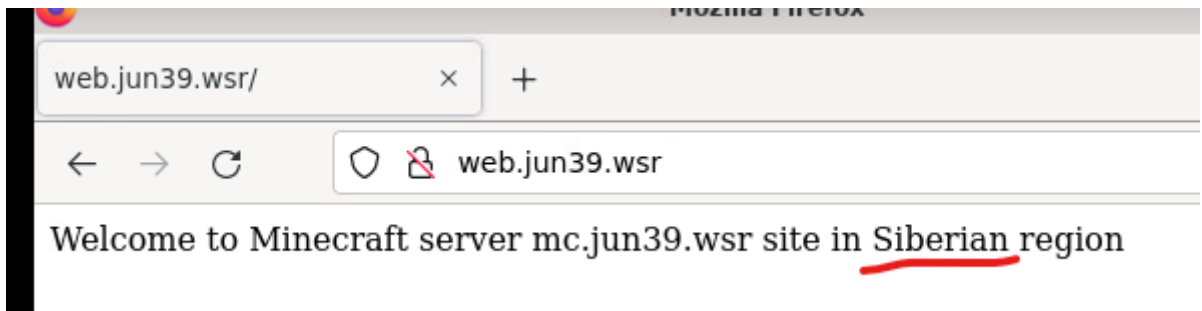


ClientVV

Меняем адрес DNS сервера с 100.100.100.100 на 100.70.6.12

Перезапускаем сетевое подключение

В браузере вводим <http://web.jun39.wsr>, должен открыться сайт с APP-ИКТ



Настройка инфраструктуры DNS для доступа к другим филиалам по доменным именам

FW-IKT

Службы 1

2 Dnsmasq DNS

3 Настройки

Переопределение хоста

Хост	Домен	IP-адрес	Описание
app-ikt	ikt.jun39.wsr	192.168.4.3	
fw-ikt	ikt.jun39.wsr	192.168.3.1	
srv1-ikt	ikt.jun39.wsr	192.168.3.2	
web	jun39.wsr	192.168.4.3	

Записи в этом разделе переопределяют отдельные результаты из Используйте их для изменения результатов DNS или добавления записей за

Переопределение домена

Домен	IP-адрес	Описание
msk.jun39.wsr	100.70.4.18	
ams.jun39.wsr	100.70.3.45	

Записи в этой зоне переопределяют целый домен, указывая полномочный DNS-сервер, который будет запрашиваться для этого домена.

4

Настройка IPSEC

<https://docs.opnsense.org/manual/how-tos/ipsec-s2s-route.html>

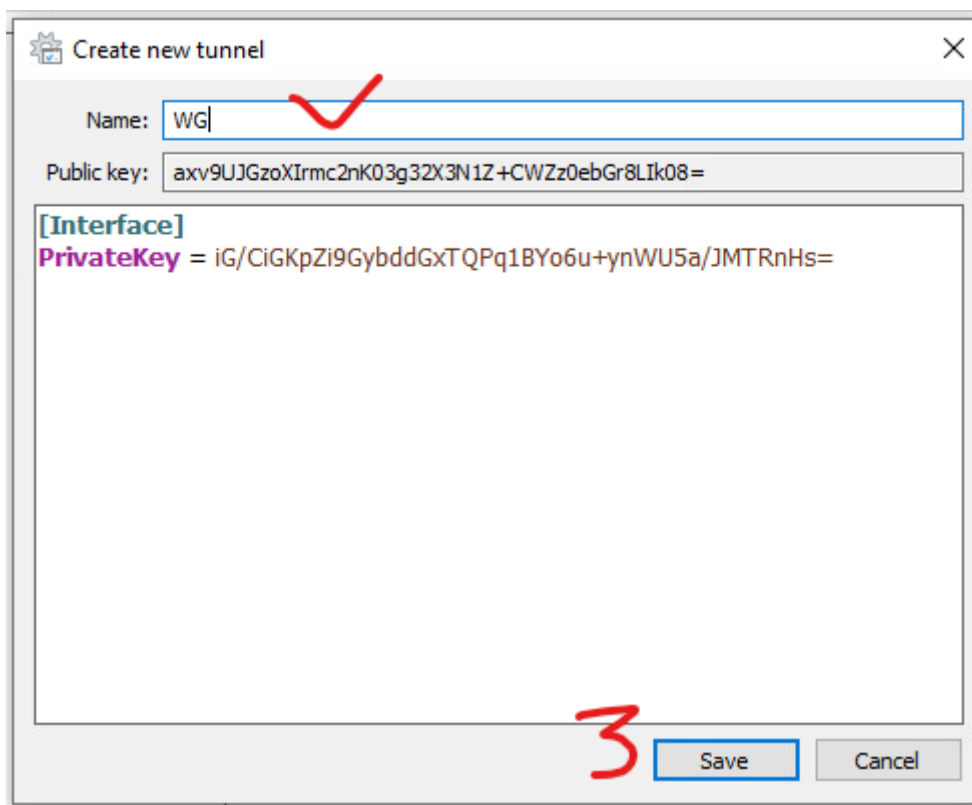
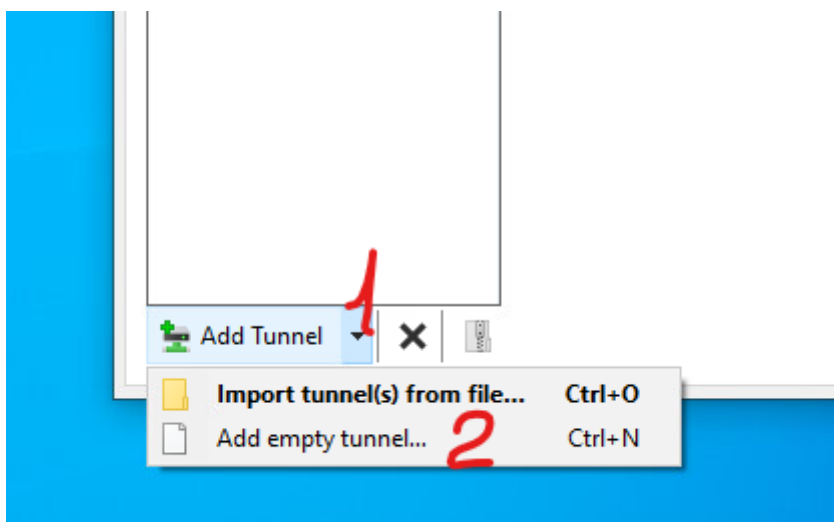
VPN

VPNClient

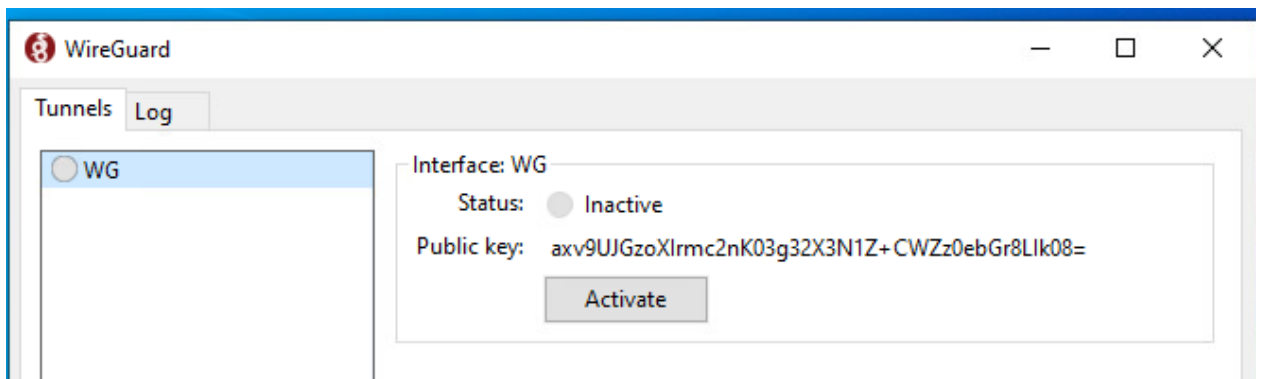
На VPNClient скачиваем и устанавливаем wireguard клиент

<https://www.wireguard.com/install/>

Запускаем Wireguard и создаем новый туннель



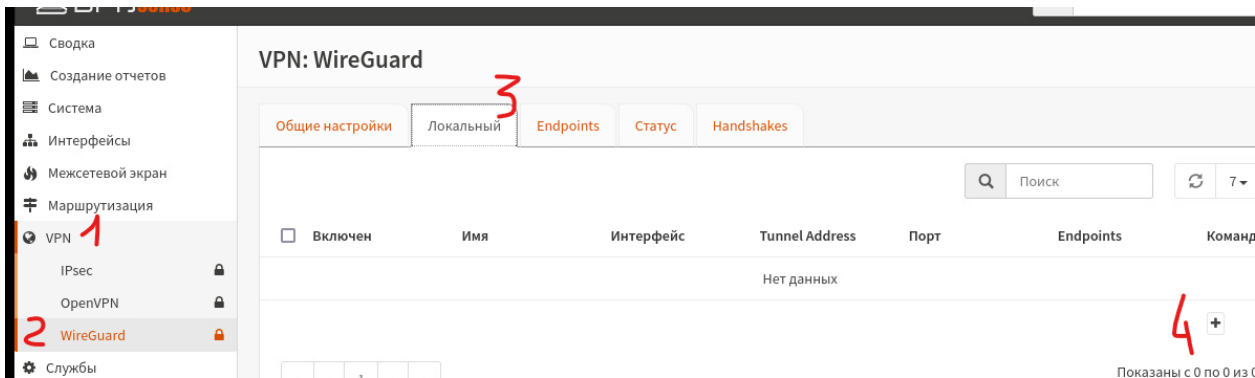
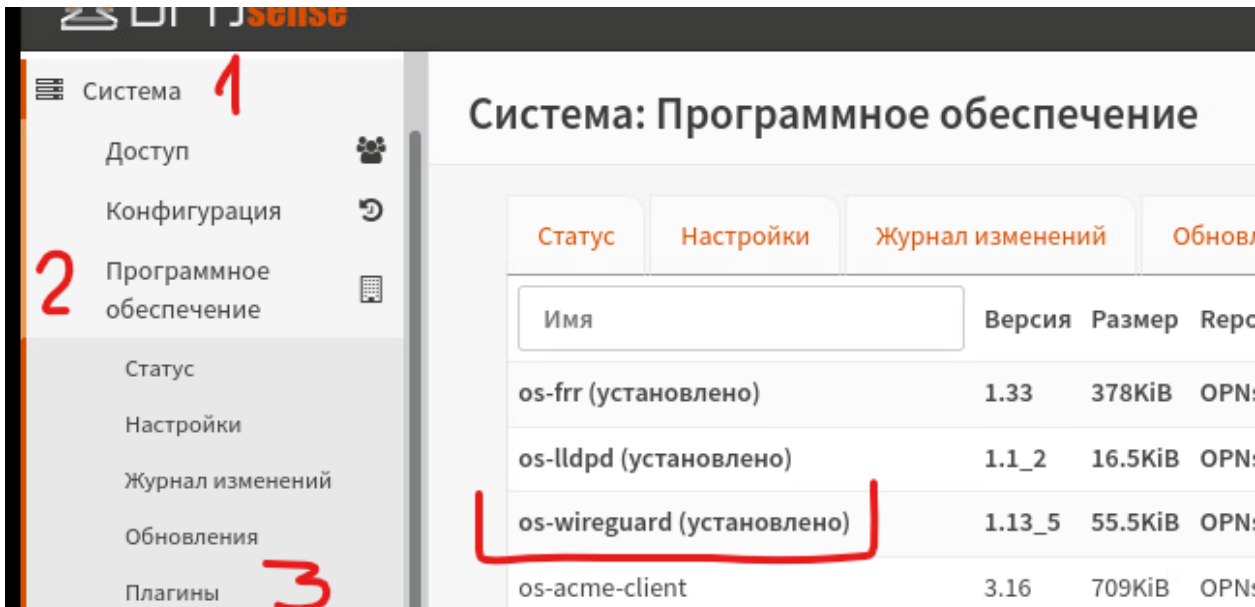
Получаем



FW-MSK

<https://docs.opnsense.org/manual/how-tos/wireguard-client.html>

Устанавливаем плагин os-wireguard



Edit Local Configuration



расширенный режим

справка

Включен



Имя

WG

Instance

1

Public Key

Private Key

Порт прослушивания

51820

Tunnel Address

10.10.12.1/24

Очистить все

Сору

Peers

Ничего не выбрано

Очистить все

Disable Routes



Отменить

Сохранить

Общие настройки

Локальный

Endpoints

Статус

Handshakes



Поиск



7



Включен

Имя

Интерфейс

Tunnel Address

Порт

Endpoints

Команды



WG

wg1

10.10.12.1/24

51820

6



✕

Edit Local Configuration

расширенный режим

справка

Включен

☒

Имя

WG

Instance

1

Public Key

QRpeUrS0mQiiEPZFIZCIhr+oJ7gOcgMVeHRYXCFWA=

✓

Private Key

iLzh+CvNPnOM6C/2rcvUctg/Y8RvIwTL6dID9UgPAFg=

Порт прослушивания

51820

Tunnel Address

10.10.12.1/24

Очистить все

Скопировать

Peers

Ничего не выбрано

Очистить все

Disable Routes

☐

Отменить

Сохранить

Нужно сохранить Public Key

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Маршрутизация

VPN

1

IPsec

OpenVPN

WireGuard

2

Службы

VPN: WireGuard

Общие настройки

Локальный

Endpoints3

Статус

Handshakes

Поиск

7

Включен	Имя	Endpoint Address	Endpoint Port	Allowed IPs	Команды
Нет данных					
4 +					

Показаны 0 из 0 записей

Edit Endpoint

справка

Включен

☒

✓

Имя

VPNClient

✓

Public Key

ixv9UJGzoXIrmc2nK03g32X3N1Z+CWZz0ebGr8LIk08=

✓

Общий секретный ключ

Allowed IPs

10.10.12.2/32

✓

Очистить все

Copy

Endpoint Address

Endpoint Port

Keepalive Interval

Отменить

Сохранить

5

ВНИМАНИЕ Public Key берется от VPNClient

Общие настройки

Локальный

Endpoints

Статус

Handshakes

Поиск

Поиск

↺

7

☰

<div><input type="checkbox"/> Включен</div>	Имя	Endpoint Address	Endpoint Port	Allowed IPs	Команды
<div><div>☐</div><div><input checked="" type="checkbox"/></div></div>	VPNClient			10.10.12.2/32	<div><div>✎</div><div>📄</div><div>🗑</div></div>
<div>+</div>					

«

<

1

>

»

Показаны с 1 по 1 из 1 записей

Применить

6

Сводка

Создание отчетов

Система

Интерфейсы

Межсетевой экран

Маршрутизация

VPN

IPsec

OpenVPN

WireGuard

Службы

Питание

Помощь

VPN: WireGuard

Общие настройкиЛокальныйEndpointsСтатусHandshakes

Поиск

7

<input type="checkbox"/>	Включен	Имя	Интерфейс	Tunnel Address	Порт	Endpoints	Команды
<input checked="" type="checkbox"/>		WG	wg1	10.10.12.1/24	51820		<div><div></div><div></div><div></div></div>

« < 1 > »

Показаны с 1 по 1 из 1 записей

Применить

Edit Local Configuration

расширенный режимсправка

Включен

Имя

Instance

Public Key

Private Key

Порт прослушивания

Tunnel Address

Peers

Disable Routes

☒

WG

1

ϰQRpeUrS0mQiiEPZFIZCIhr+oJ7gOcgMVeHRYXCFWA=

iLzh+CvNPnOM6C/2rcvUctg/Y8RvlwTL6dID9UgPAFg=

51820

10.10.12.1/24

Очистить все

Скопировать

VPNClient

☒ VPNClient

Отменить

Сохранить

VPN: WireGuard

Сводка
Создание отчетов
Система
Интерфейсы
Межсетевой экран
Маршрутизация
VPN 1
IPsec
OpenVPN
2 WireGuard
Службы

Общие настройки 3 Локальный Endpoints Статус

Enable WireGuard 4 ☒

Применить 5

Интерфейсы: Назначения портов

Создание отчетов
Система
Интерфейсы 1
[DMZ]
[IPSEC2]
[IPSEC3]
[LAN]
[WAN]
2 Назначения портов
Обзор
Настройки
Виртуальные IP-адреса
Беспроводные сети
Point-to-Point
Другие типы
Диагностика
Межсетевой экран

Интерфейс (ID ?)	Сетевой порт	
DMZ (opt1)	vmx2 (00:0c:29:3d:6c:fc)	
IPSEC2 (ipsec2)	ipsec2 ()	
IPSEC3 (ipsec3)	ipsec3 ()	
LAN (lan)	vmx0 (00:0c:29:3d:6c:e8)	
WAN (wan)	vmx1 (00:0c:29:3d:6c:f2)	
Новый интерфейс:	wg1 (00:00:00:00:00:00)	+
Описание	WG	

✓

Сохранить 4

Интерфейсы: [WG]

Создание отчетов
Система
Интерфейсы 1
[DMZ]
[IPSEC2]
[IPSEC3]
[LAN]
[WAN]
2 [WG]
Назначения портов
Обзор
Настройки

Basic configuration

Включен ☒ Включить интерфейс 3

Блокировать ☐ Предотвращение удаления интерфейса

Устройство wg1

Описание WG

Generic configuration

Блокировать частные сети ☐

Hardware settings

Overwrite global settings

☐

4

Сохранить

Отменить

5

Применить изменения

1

Правила

Floating

DMZ

IPsec

IPSEC2

IPSEC3

LAN

Loopback

WAN

WG

WireGuard (Group)

Ограничитель трафика

Настройки

Межсетевой экран: Правила: WG

Выберите категорию

Inspect

No WG rules are currently defined. All incoming connections on this interface will be blocked until you add a pass rule. Exceptions for automatically generated rules may apply.

3

+

←

🗑️

☑️

□

Протокол

Источник

Порт

Назначение

Порт

Шлюз

Расписание

Описание

Automatically generated rules

31

▶️ разрешение

❌ блокирование

⚠️ отклонение

📄 журналирование

→ входящий

⚡ первое совпадение

▶️ разрешение (отключено)

❌ блокирование (отключено)

⚠️ отклонение (отключено)

📄 журналирование (отключено)

← исходящий

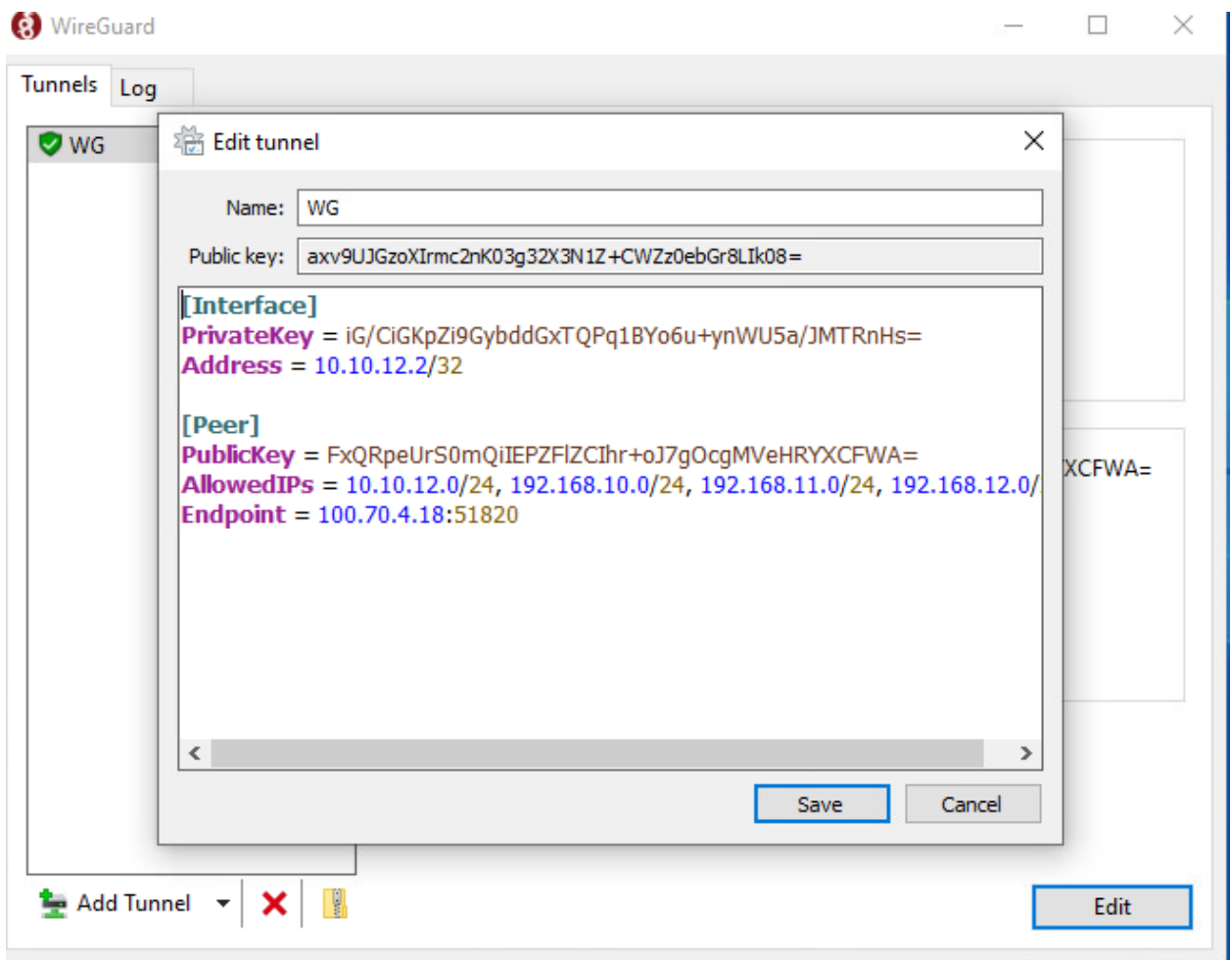
⚡ последнее совпадение

📅 Active/Inactive Schedule (click to view/edit)

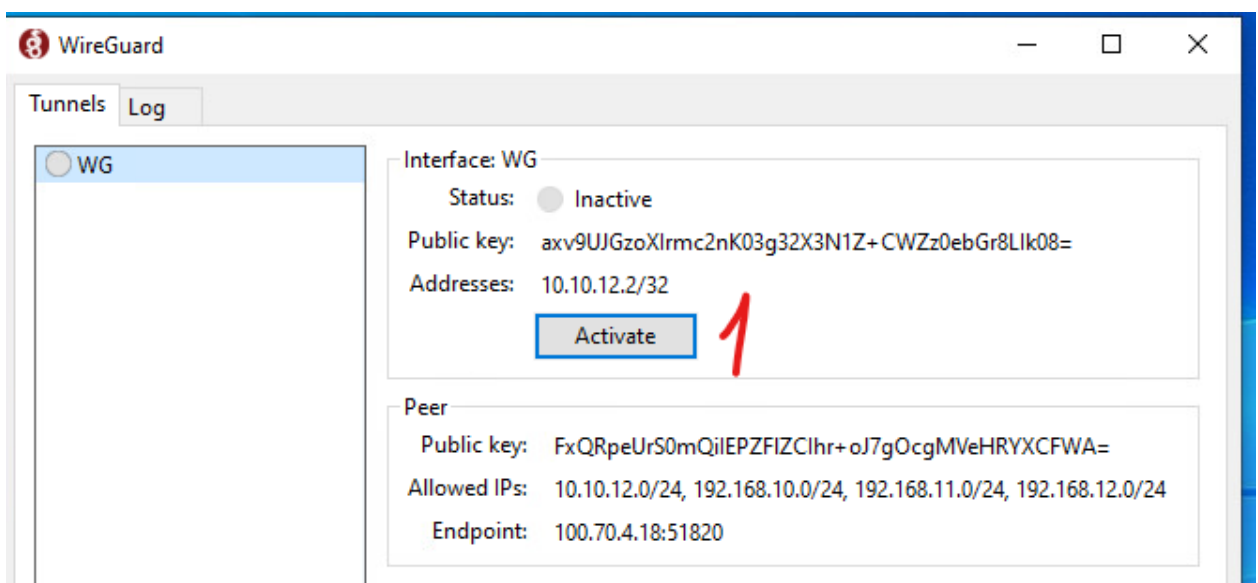
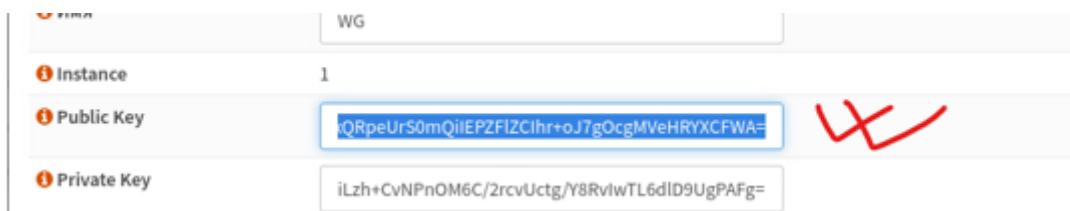
📄 Псевдоним (нажмите для просмотра/редактирования)

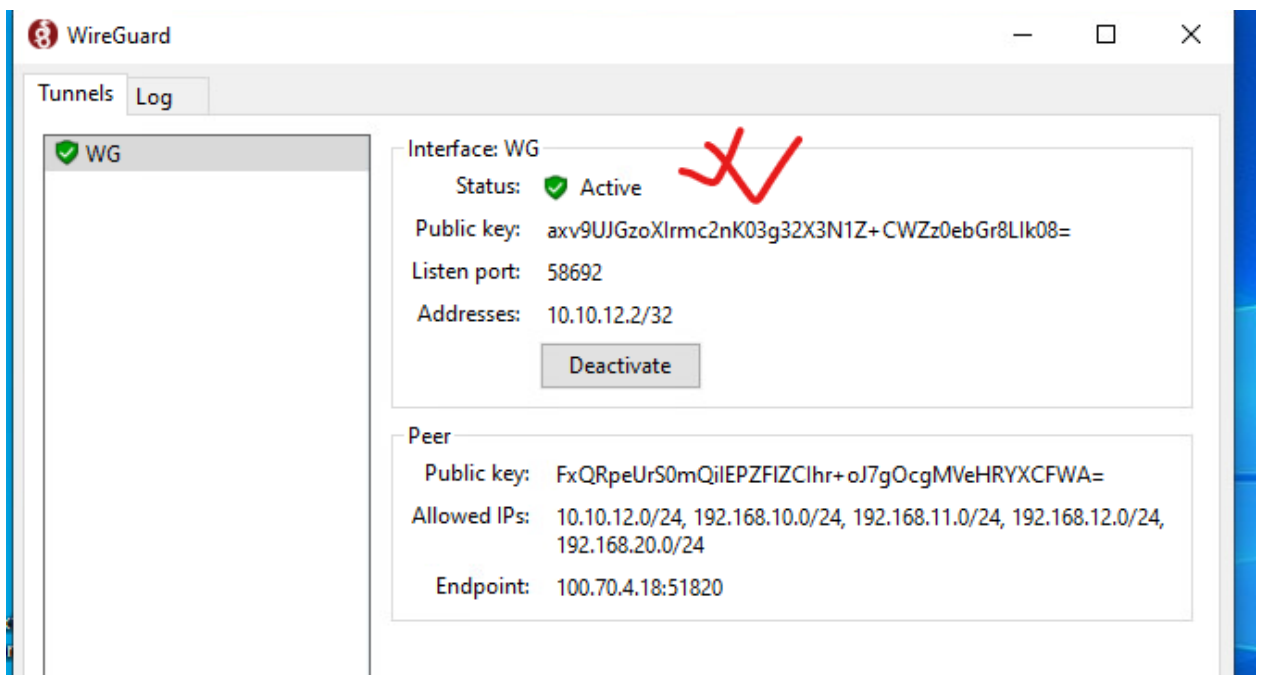
	Протокол	Источник	Порт	Назначение	Порт	Шлюз	Расписание	Описание	
	Automatically generated rules								31
	IPv4 *	*	*	*	*	*	*		<div>←</div> <div>✎</div> <div>📄</div> <div>🗑️</div>
▶️	разрешение	❌		⚠️				→ входящий	⚡
▶️	разрешение (отключено)	❌		⚠️				← исходящий	⚡
								первое совпадение	
								последнее совпадение	

На VPNClient



Где [Peer] PublicKey = Публичный ключ FW





Проверка

ping 192.168.12.2

ping 192.168.12.3

ping 192.168.20.2

Настройка журналирования

SRV1-MSK

```
mkdir /opt/logs
```

```
chmod 777 /opt/logs/
```

```
nano /etc/rsyslog.conf
```

#Раскомментируем 2 строчки (убирает #)

```
module(load="imudp")
```

```
input(type="imudp port="514")
```

```
module(load="imtcp")
```

```
input(type="imtcp port="514")
```

В добавляем

```
$template RemoteLogs, "/opt/log/%HOSTNAME%/%HOSTNAME%.log"
```

```
*.* ?RemoteLogs
```

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

$template RemoteLogs, "/opt/logs/%HOSTNAME%/%HOSTNAME%.log"
*.* ?RemoteLogs
```

```
systemctl restart rsyslog
```

```
systemctl status rsyslog
```

SRV2-MSK

```
nano /etc/rsyslog.conf
```

В конце файла добавляем

```
*.warn @192.168.12.2
```

```
systemctl restart rsyslog
```

```
systemctl status rsyslog
```

Проверка

```
logger -p local4.warn "Warning SRV2-MSK"
```

PC-MSK

```
nano /etc/rsyslog.conf
```

В конце файла добавляем

```
*.err @192.168.12.2
```

```
systemctl restart rsyslog
```

```
systemctl status rsyslog
```

Проверка

```
logger -p local4.err "Error PC-MSK"
```

FW-MSK

Сводка
Создание отчетов
Система 1
Доступ
Конфигурация
Программное обеспечение
Шлюзы
Высокий уровень доступности
Маршруты
Настройки 2
Администрирование
Планирование задач Cron
Общие настройки
Журналирование
Logging / targets 3
Прочее

Система: Настройки: Logging / targets

Получатели **Статистические данные**

Поиск

☐ Включен Транспортный протокол Имя хоста Описание Команды

Нет данных

« < 1 > »

Применить

4 + -

Показаны с 0 по 0 из 0 записей

Edit destination

Включен ☒

Транспортный протокол UDP(4)

Applications ipsec (charon), routing (ospfd) ✓

✖ Очистить все

Levels notice, warn, error, критический, alert, emergency ✓

✖ Очистить все

Facilities Ничего не выбрано

✖ Очистить все

Имя хоста 192.168.12.2 ✓

Порт 514

rfc5424 ☐

Описание